Tartu Ülikool

Loodus- ja täppisteaduste valdkond

Matemaatika ja statistika instituut

Alvin Lepik

Poolrühmade põimikkorrutis ja Krohn-Rhodes'i teoreem

Matemaatika eriala

Bakalaureusetöö (9 EAP)

Juhendaja : Valdis Laan

Tartu 2017

Poolrühmade põimikkorrutis ja Krohn-Rhodes'i teoreem

Bakalaureusetöö

Alvin Lepik

Lühikokkuvõte. Bakalaureusetöös vaadeldakse poolrühmi. Töö eesmärgid on täpsustada põimikkorrutise mõiste poolrühmade korral, esitada mõned poolrühmade põimikkorrutise omadused, nende tõestused ja, põhieesmärgina, tõestada Krohn-Rhodes'i teoreem teatud tüüpi lõplike poolrühmade ehituse kohta. Töö põhineb peamiselt Pierre Antoine Grillet' monograafial *Semigroups: An Introduction to the Structure Theory (Tulane Ülikool, New York, 1995)*.

CERCS teaduseriala: P120 Arvuteooria, väljateooria, algebraline geomeetria, algebra, rühmateooria
Märksõnad: homomorfism, poolrühmade põimikkorrutis, poolrühmade jaguvus

Wreath product of semigroups and the Krohn-Rhodes theorem

Bachelor's thesis

Alvin Lepik

Abstract. The objects of study in this bachelor thesis are semigroups. The objectives are to specify the notion of wreath product of semigroups, to present and prove some properties of wreath product of semigroups and, as the main objective, to prove the Krohn-Rhodes theorem on the structure of certain kind of finite semigroups. The thesis is largely based on Pierre Antoine Grillet's monograph *Semigroups: An Introduction to the Structure Theory (Tulane University, New York, 1995)*.

CERCS specialization: P120 Number theory, field theory, algebraic geometry, algebra, group theory
Keywords: homomorphism, wreath product of semigroups, divisibility of semigroups

Sisukord

Sissejuhatus

Käesoleva bakalaureusetöö valdkond on algebra. Valdavalt tutvustatakse mõisteid poolrühmateooriast, aga ka elemente rühmateooriast. Bakalaureusetöö on referatiivne. Töö põhineb P. A. Grillet' monograafial [G]. Lisaks kasutatakse M. Kilbi algebra õpikuid [K1] ja [K2] ning J. Howie raamatut [H]. Eeldatakse, et lugejale on selged hulgateooria põhimõisted ja lausearvutus.

Töö koosneb kolmest osast. Esimeses osas tuletatakse meelde algebra põhikursusest teada olevad mõisted ning esitatakse ka piisavalt teooriaelemente nii poolrühma- kui ka rühmateooriast, sealjuures tõestatakse olulised abitulemused, mida kasutatakse töö teises ja kolmandas osas.

Teises osas täpsustatakse poolrühmade jaguvuse ja põimikkorrutise mõisted ja tõestatakse mõned nendega seonduvad omadused.

Kolmas osa on pühendatud käesoleva töö põhiteoreemiga seonduvatele abitulemustele ja põhiteoreemile, milleks on järgmine väide.

Teoreem (Krohn-Rhodes)**.** *Iga lõplik poolrühm S jagab lõplikku põimikkorrutist, mis on saadud lihtsatest rühmadest, mis jagavad poolrühma S või parempoolse korrutamisega kahe-elemendilistest poolrühmadest, millel on väliselt lisatud ühikelement.*

1965. aastal avaldasid Kenneth Krohn ja John Rhodes artikli [KRA], milles on tõestatud väide lõplike poolrühmade ehituse kohta. Krohn'i ja Rhodes'i ühistöö tulemusena sai alguse distsipliin, mida tänapäeval tuntakse kui Krohn-Rhodes'i teooriat, sealjuures käesolevas töös esitatud teoreem on Krohn-Rhodes'i teooria alustalaks, millele muuhulgas leidub rakendus mänguteoorias (vt [KRT]).

Bakalaureusetöös reprodutseeritud Krohn-Rhodes'i teoreemi tõestus järgib Grillet' monograafias [G] esitatud tõestust. Osutub, et ühe olulise väitega seonduv tõestus on raamatus [G] poolik tänu millele pole võimalik Krohn-Rhodes'i teoreemi Grillet' monograafia põhjal täielikult ära tõestada.

Põhimõisted

Poolrühmaks nimetatakse paari $(S, \cdot) =: S$, kus S on mittetühi hulk ja on defineeritud kahekohaline algebraline tehe

$$\cdot : S \times S \to S, (a, b) \mapsto a \cdot b,$$

mis on assotsiatiivne st iga $a, b, c \in S$ korral

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

Sellist tehet nimetatakse korrutamiseks ning iga $a, b \in S$ korral kirjutatakse harilikult $a \cdot b =: ab$. Elementi $ab \in S$ nimetatakse elementide a ja b korrutiseks.

Kui leidub element $e \in S$ nii, et mistahes $x \in S$ korral $ex = xe = x$, siis öeldakse, et e on poolrühma S **ühikelement** ja tähistatakse sümboliga 1_S või lihtsalt 1. Lihtne on mõista, et poolrühma ühikelement, kui ta leidub, on üheselt määratud. Poolrühma, mis sisaldab ühikelementi, nimetatakse **monoidiks**. Kui mingi monoidi elemendi $s \in S$ korral leidub $t \in S$ omadusega $st = ts = 1$, siis öeldakse, et element s on **pööratav**, seejuures elementi t nimetatakse elemendi s **pöördelemendiks**, mida harilikult tähistatakse kirjutisega s^{-1}. Monoidi, mille iga element on pööratav, nimetatakse **rühmaks**.

Poolrühma $(S, \cdot)$ alamhulka S' nimetatakse **alampoolrühmaks**, kui $(S', \cdot)$ on poolrühm. Alamhulk $S' \subseteq S$ on **alammonoid**, kui $(S', \cdot)$ on monoid. Alamhulka $G' \subseteq S$ nimetatakse **alamrühmaks**, kui $(G', \cdot)$ on rühm.

Lihtne on veenduda, et hulk $S' \subseteq S$ on alampoolrühm parajasti siis, kui S' on kinnine korrutamise suhtes ehk

$$(\forall x, y \in S')\,(xy \in S')\,.$$

Oleme harjunud kujutuse $f : A \to B$ korral elemendi $a \in A$ kujutist tähistama kirjutisega $f(a)$. Edaspidi, kirjutame $af := f(a)$ ning hulga A kujutist tähistame

kirjutisega Af. Kui

$$f : A \to B \quad \text{ja} \quad g : B \to C$$

on kujutused, siis nende järjestrakenduse ehk kompositsiooni korral $fg : A \to C$ ja $a(fg) = (af)g$.

Ehkki üldiselt poolrühmas ei ole ühikelementi, osutub tihti kasulikuks opereerida monoidis, seega, kui S ei ole monoid, defineeritakse monoid S^1 nii, et

$$S^1 := S \sqcup \{1\},$$

kus iga $s \in S$ korral $s1 = 1s = s$ ja $11 = 1$. Öeldakse, et monoid S^1 on saadud poolrühmast S välise ühikelemendi lisamisel.

Kui $x \in S$ ja $k \in \mathbb{N}$, siis kasutatakse tähistust

$$x^k := \underbrace{x\,x\,\ldots\,x}_{k \text{ tegurit}}.$$

On selge, et iga $k, l \in \mathbb{N}$ korral $x^{k+l} = x^k \cdot x^l$ ja $(x^k)^l = x^{kl}$.

Olgu S poolrühm ja $A, B \subseteq S$ mingid mittetühjad hulgad. Kirjutisega AB peetakse silmas hulka $\{ab : a \in A, b \in B\}$. Kui A on üheelemendiline hulk $\{a\}$, siis hulka $\{a\}\,B$ tähistatakse aB. Analoogiliselt $Ab = A\,\{b\}$.

Mittetühja hulka $I \subseteq S$ nimetatakse **vasakpoolseks ideaaliks** poolrühmas S, kui $SI \subseteq I$, **parempoolseks ideaaliks** poolrühmas S, kui $IS \subseteq I$. Hulk I on **ideaal** poolrühmas S, kui $SIS \subseteq I$. Lihtne on veenduda, et I on ideaal poolrühmas S parajasti siis, kui I on vasak- ja parempoolne ideaal poolrühmas S, kusjuures iga $a \in S^1$ korral S^1a on vasakpoolne ideaal, aS^1 on parempoolne ideaal ja S^1aS^1 on ideaal poolrühmas S.

Käesolevas töös tähistab S kõikjal poolrühma, kui just ei ole öeldud teisiti.

1.1 Kongruentsid ja Greeni seosed

Definitsioon. Olgu A mingi mittetühi hulk. Öeldakse, et seos $\rho \subseteq A \times A$ on **eeljärjestus**, kui ρ on refleksiivne ja transitiivne.

Kui ρ on eeljärjestus hulgal A, siis defineerides seose $\hat{\rho}$ nii, et iga $a, b \in A$ korral

$$a\hat{\rho}b \iff a\rho b \quad \text{ja} \quad b\rho a,$$

saame ekvivalentsiseose hulgal A. Edaspidi tähistame ekvivalentsiseoseid suurte kirjatähtedega: $\mathscr{A}, \mathscr{B}, \mathscr{C}$ jne.

Definitsioon. Olgu $\mathscr{C} \subseteq S \times S$ ekvivalentsiseos. Öeldakse, et $\mathscr{C}$ on **vasakpoolne kongruents** poolrühmal S, kui iga $x \in S$ korral

$$a \mathscr{C} b \Longrightarrow xa \mathscr{C} xb \qquad (a, b \in S).$$

Analoogiliselt defineeritakse parempoolne kongruents poolrühmal S. Ekvivalentsiseost $\mathscr{C}$ nimetatakse **kongruentsiks** poolrühmal S, kui $\mathscr{C}$ on vasak- ja parempoolne kongruents poolrühmal S. Pole ka raske veenduda, et poolrühma S kongruentside suvaline ühisosa on samuti kongruents poolrühmal S.

Definitsioon. Olgu elemendid $a, b \in S$. **Greeni eeljärjestusteks** poolrühmal S nimetatakse seoseid $\leq_{\mathscr{L}}, \leq_{\mathscr{R}}, \leq_{\mathscr{H}}, \leq_{\mathscr{J}}$, mis on defineeritud

$$\begin{aligned}
a \leq_{\mathscr{L}} b &\iff \exists u \in S^1 : a = ub \qquad \iff S^1 a \subseteq S^1 b, \\
a \leq_{\mathscr{R}} b &\iff \exists v \in S^1 : a = bv \qquad \iff a S^1 \subseteq b S^1, \\
a \leq_{\mathscr{H}} b &\iff a \leq_{\mathscr{L}} b \quad \text{ja} \quad a \leq_{\mathscr{R}} b \iff S^1 a \subseteq S^1 b \text{ ja } a S^1 \subseteq b S^1, \\
a \leq_{\mathscr{J}} b &\iff \exists u, v \in S^1 : a = ubv \iff S^1 a S^1 \subseteq S^1 b S^1.
\end{aligned}$$

Lähtuvalt Greeni eeljärjestustest, defineeritakse Greeni seosed poolrühmal S.

Definitsioon. Olgu elemendid $a, b \in S$. **Greeni seosteks** poolrühmal S nimetatakse seoseid $\mathscr{L}, \mathscr{R}, \mathscr{H}, \mathscr{J}$, mis on defineeritud

$$\begin{aligned}
a \mathscr{L} b &\iff a \leq_{\mathscr{L}} b \quad \text{ja} \quad b \leq_{\mathscr{L}} a, \\
a \mathscr{R} b &\iff a \leq_{\mathscr{R}} b \quad \text{ja} \quad b \leq_{\mathscr{R}} a, \\
a \mathscr{H} b &\iff a \leq_{\mathscr{H}} b \quad \text{ja} \quad b \leq_{\mathscr{H}} a, \\
a \mathscr{J} b &\iff a \leq_{\mathscr{J}} b \quad \text{ja} \quad b \leq_{\mathscr{J}} a.
\end{aligned}$$

Kuna eelnevad neli Greeni seost on sümmeetrilised eeljärjestused, siis nad on ekvivalentsiseosed. Tähistatakse esindajaga $x \in S$ $\mathscr{J}$-klassi sümboliga J_x, seega $J_x \subseteq S$ ja saame faktorhulga

$$S/\mathscr{J} = \{J_x : x \in S\}.$$

Analoogiliselt tähistatakse ekvivalentsiklasse ka teiste Greeni seoste puhul. Tuleb välja, et eeljärjestus $\leq_{\mathscr{J}}$ indutseerib osalise järjestuse hulgas $S/\mathscr{J}$.

Lause 1.1.1. *Olgu elemendid $a, b \in S$. Siis seos $\leq$ hulgas $S/\mathscr{J}$, mis on defineeritud*

$$J_a \leq J_b \iff a \leq_{\mathscr{J}} b,$$

on osaline järjestusseos.

Tõestus. Kuna seos $\leq_{\mathscr{J}}$ on eeljärjestus, siis seos $\leq$ on refleksiivne ja transitiivne. Kui $J_a \leq J_b$ ja $J_b \leq J_a$, siis leiduvad $u, v, t, w \in S^1$ sellised, et

$$a = ubv \quad \text{ja} \quad b = taw,$$

järelikult kehtivad sisalduvused

$$S^1aS^1 \subseteq S^1bS^1 \quad \text{ja} \quad S^1bS^1 \subseteq S^1aS^1,$$

millest saame, et $S^1aS^1 = S^1bS^1$ ehk $a \mathscr{J} b$, seega $J_a = J_b$, mis tähendab, et seos $\leq$ on antisümmeetriline. ■

Samuti, lihtne on veenduda, et lause 1.1.1 väitega analoogilised väited kehtivad faktorhulkades $S/\mathscr{L}$, $S/\mathscr{R}$ ja $S/\mathscr{H}$. Lepime kokku, hulgas $S/\mathscr{J}$, ranget järjestust $J_a < J_b$ mõista kui asjaolu, et $J_a \leq J_b$ ja $J_a \neq J_b$ st mistahes elementide $a, b \in S$ korral

$$J_a < J_b \iff S^1aS^1 \subset S^1bS^1.$$

Kehtigu ka analoogilised kokkulepped faktorhulkades $S/\mathscr{L}$, $S/\mathscr{R}$, $S/\mathscr{H}$. Ilmsed on faktid, et $\mathscr{L}$ on parempoolne kongruents ja $\mathscr{R}$ on vasakpoolne kongruents poolrühmal S. Greeni seoste peamine omadus on kirjeldatav järgmise tulemusega, mis on esitatud monograafias [G] tulemusena II.1.3.

Lemma 1.1.2 (Greeni lemma). *Olgu $a, b \in S$ nii, et $a\mathscr{L}b$ ehk leiduvad $u, v \in S^1$ nii, et $b = ua$ ja $a = vb$. Siis kujutused*

$$f : R_a \to R_b, \quad x \mapsto ux \quad \textit{ja} \quad g : R_b \to R_a, \quad y \mapsto vy$$

on teineteise pöördkujutused, mis säilitavad $\mathscr{L}$-klassid.

Tõestus. Väite tõestuseks piisab näidata, et fg ja gf on samasusteisendused. Olgu $x \in R_a$ suvaline. Et $\mathscr{R}$ on vasakpoolne kongruents, siis $ux \in R_{ua} = R_b$. Analoogilise arutelu põhjal, kuna $y \in R_b$, siis $vy \in R_{vb} = R_a$. Leidub $s \in S^1$ nii, et $x = as$ ning

$$x(fg) = (xf)g = (ux)g = vux = vuas = vbs = as = x,$$

kusjuures märkame, et $x = v(ux)$ ehk $x \leq_{\mathscr{L}} ux$. Triviaalselt kehtib $ux \leq_{\mathscr{L}} x$, seega kokku saame $x\mathscr{L}ux$. Analoogiliselt on põhjendatav asjaolu, et $y(gf) = y$ ning $vy\mathscr{L}y$. Sellega oleme näidanud, et f ja g on bijektsioonid, teineteise pöördkujutused ning veendunud, et f ja g säilitavad $\mathscr{L}$-klassid. ■

Analoogiliselt saab veenduda Greeni lemma (lemma 1.1.2) nn "duaalse" väite õigsuses.

Järeldus. *Olgu $a, b \in S$ nii, et $a\mathscr{R}b$ ehk leiduvad $u, v \in S^1$ omadusega $b = au$ ja $a = bv$. Siis kujutused*

$$f : L_a \to L_b, \quad x \mapsto xu \quad \textit{ja} \quad g : L_b \to L_a, \quad y \mapsto yv$$

on teineteise pöördkujutused, mis säilitavad $\mathscr{R}$-klassid.

Kui ρ ja τ on mingid seosed ja tahame väljendada, et $a\rho b$ ja $b\tau c$, siis kirjutame $a\rho b\tau c$. Eraldi mainimist väärib järgmine omadus.

Lemma 1.1.3. *Greeni seos $\mathscr{H}$ on kongruents.*

Tõestus. Näitamaks, et $\mathscr{H}$ on kongruents, peame näitama, et $\mathscr{H}$ on vasak- ja parempoolne kongruents poolrühmal S. Olgu $x, y \in S$ ja $x\mathscr{H}y$. Kuna $\mathscr{R}$ on vasakpoolne kongruents, siis iga $u \in S$ korral $ux\mathscr{R}uy$. Teisalt, lemma 1.1.2 põhjal, $ux\mathscr{L}x\mathscr{L}y\mathscr{L}uy$, järelikult $ux\mathscr{H}uy$. Analoogiliselt on põhjendatav, et iga $u \in S$ korral $xu\mathscr{H}yu$. ■

Kasulikuks osutub järgmine fakt.

Lause 1.1.4 ([G] I.3). *Kui $\mathscr{C}$ on kongruents poolrühmal S, siis $S/\mathscr{C}$ on poolrühm.*

Tõestus. Defineerime korrutamise $*$ hulgal $S/\mathscr{C}$ esindajate kaudu st iga $a, b \in S$ korral

$$C_a * C_b = C_{ab}.$$

Näitame, et tulemus ei sõltu esindajate valikust. Olgu $a\mathscr{C}x$ ja $b\mathscr{C}y$, kus $x, y \in S$. Kuna $\mathscr{C}$ on kongruents, siis $ab\mathscr{C}xb\mathscr{C}xy$, millest transitiivsuse tõttu $ab\mathscr{C}xy$ ehk $C_{ab} = C_{xy}$. Olgu $a, b, c \in S$, siis

$$(C_a * C_b) * C_c = C_{ab} * C_c = C_{(ab)c} = C_{a(bc)} = C_a * (C_b * C_c),$$

millega oleme näidanud, et tehe $*$ on assotsiatiivne. ■

Definitsioon. Poolrühma S elementi x nimetatakse **idempotendiks**, kui $x^2 = x$. Poolrühma S idempotentide hulka tähistatakse $E(S)$.

Hulgal $E(S)$ defineeritakse osaline järjestusseos $\leq$ nii, et iga $e, f \in E(S)$ korral

$$e \leq f \iff e \leq_{\mathscr{H}} f \iff ef = fe = e$$

(vt [G] II.1.1). Olukorra $e < f$ all mõistame asjaolu, et $ef = fe = e$ ja $e \neq f$.

Lause 1.1.5 ([G] II.1.4). *Olgu H poolrühma S $\mathscr{H}$-klass, siis järgmised väited on samaväärsed.*

(a) Leiduvad $a, b \in H$ nii, et $ab \in H$.

(b) Hulgas H leidub idempotent.

(c) H on poolrühma S alamrühm.

Tõestus. Kui H on alamrühm, siis ühikelement $1_H \in H$ ja 1_H on idempotent. Näitame kõigepealt, et väitest (a) järeldub (b).

Olgu $a, b \in H$ ja $ab \in H$, siis $ab\mathscr{L}b$ ja Greeni lemma põhjal (vt lemma 1.1.2) kujutus

$$H_b \to H_{ab}, \quad x \mapsto ax$$

on bijektsioon, kusjuures $H_a = H_b = H_{ab} = H$, järelikult $aH = H$. Nüüd iga $c \in H$ korral $ac\mathscr{R}a$. Olgu $c \in H$ suvaline, siis Greeni lemma põhjal $Hc = H$, millest järeldub, et $H \subseteq S$ on alampoolrühm.

Kuna $Ha = H$, siis leidub $e \in H$ nii, et $a = ea$, kusjuures $ea = eea$, seega $ee = e$. Järelikult iga $x \in H$ korral $eex = ex$ ja $xe = xee$, millest järeldub, et $ex = xe = x$, seega H on monoid ühikelemendiga e, millega oleme näidanud, et kehtib väide (b).

Näitame, et väitest (b) järeldub (c). Olgu $c \in H$ suvaline. Greeni lemma põhjal kujutused

$$H \to H, \quad x \mapsto xc \quad \text{ja} \quad y \mapsto cy$$

on bijektsioonid, järelikult leiduvad $x, y \in H$ nii, et $xc = cy = e$, kusjuures

$$x = xe = x(cy) = (xc)y = ey = y,$$

seega c on pööratav ja H on rühm. ■

Poolrühma S alamrühm $H \subseteq S$ on **maksimaalne alamrühm**, kui mistahes alamrühma $G \subseteq S$ korral

$$H \subseteq G \Longrightarrow H = G.$$

Lihtne on mõista, et kui $G \subseteq S$ on alamrühm, siis iga $f, g \in G$ korral $f\mathscr{H}g$. Lausest 1.1.5 järeldub, et on üksühene vastavus poolrühma S maksimaalsete alamrühmade ja idempotenti sisaldavate $\mathscr{H}$-klasside vahel. Järelikult poolrühma S maksimaalsed alamrühmad on paarikaupa lõikumatud ning iga alamrühm $G \subseteq S$ sisaldub täpselt ühes maksimaalses alamrühmas (vt [G] II.1.5).

Lause 1.1.6 ([G] II.1.2). *Greeni seosed $\mathscr{L}$ ja $\mathscr{R}$ kommuteeruvad ehk iga $a, b \in S$ korral*

$$(\exists x \in S)\,(a\mathscr{L}x\mathscr{R}b) \iff (\exists y \in S)\,(a\mathscr{R}y\mathscr{L}b)\,.$$

Tõestus. Olgu $a\mathscr{L}x\mathscr{R}b$ mingi $x \in S$ korral, siis leiduvad $u, v, r, s \in S^1$ nii, et

$$a = ux, \quad x = va, \quad x = br \quad \text{ja} \quad b = xs.$$

Nüüd kehtivad asjaolud, et $u(xs) = (ux)s = as$ ja

$$a = ux = u(br) = u(xs)r = (uxs)r,$$

millest saame, et $a\mathscr{R}uxs$. Teisalt, et $uxs = ub$ ja $b = xs = vas = v(uxs)$, siis $uxs\mathscr{L}b$ ja kokku saame $a\mathscr{R}(uxs)\mathscr{L}b$.

Teisalt, kui leidub $y \in S$ omadusega $a\mathscr{R}y\mathscr{L}b$, siis lihtne on mõista, et see on samaväärne olukorraga $b\mathscr{L}y\mathscr{R}a$ ning oleme juba näidanud, et leidub $x \in S$ omadusega $b\mathscr{R}x\mathscr{L}a$. ■

On olemas ka viies Greeni seos $\mathscr{L}\mathscr{R} = \mathscr{R}\mathscr{L} =: \mathscr{D}$. Võime lause 1.1.6 põhjal defineerida

$$a\mathscr{D}b \iff (\exists x \in S)\,(a\mathscr{L}x\mathscr{R}b) \quad (a, b \in S).$$

Lihtne on mõista, et tegemist on ekvivalentsiseosega. Kuna aga ei eksisteeri eeljärjestust $\mathscr{D}$ suhtes, siis hulk $S/\mathscr{D}$ üldiselt ei ole osaliselt järjestatud.

Definitsioon. Poolrühma S elementi a nimetatakse **regulaarseks**, kui leidub $x \in S$ nii, et $a = axa$.

Lemma 1.1.7 ([G] II.2.2). *Olgu $a \in S$, siis järgmised väited on samaväärsed.*

(a) Element $a \in S$ on regulaarne.

(b) Leidub idempotent klassis R_a.

(c) Leidub idempotent klassis L_a.

Tõestus. Olgu $a \in S$ ja leidugu $x \in S$ omadusega $a = axa$. Tähistame $xax =: b$, siis $aba = a$ ja $bab = b$. Kohe on selge, et $ab \in R_a \cap L_b$, kusjuures siis

$$abab = (aba)b = ab$$

ehk $ab \in R_a$ on idempotent. Analoogiliselt $ba \in R_b \cap L_a$ ja $ba \in L_a$ on idempotent. Sellega oleme näidanud, et väitest (a) järelduvad väited (b) ja (c).

Kui leidub idempotent $e \in R_a$, siis leiduvad $u, v \in S^1$ omadusega $e = au$ ja $a = ev$, millest

$$a(ue)a = (au)ea = eea = ea = e(ev) = (ee)v = ev = a$$

ehk leidub $x \in S$ omadusega $axa = a$. Analoogiliselt, kui leidub idempotent $f \in L_a$, siis leidub $y \in S$ omadusega $aya = a$. Sellega oleme näidanud, et väitest (b) järeldub (a) ja väitest (c) järeldub (a). ■

1.2 Homomorfismid ja rühmad

Käesolevas paragrahvis olgu T poolrühm.

Definitsioon. Kujutust $\varphi : S \to T$ nimetatakse **poolrühmade homomorfismiks**, kui iga $s, s' \in S$ korral

$$(ss')\varphi = (s\varphi)(s'\varphi).$$

Bijektiivset homomorfismi nimetatakse **isomorfismiks**. Poolrühmad S ja T on **isomorfsed** ($S \cong T$), kui leidub isomorfism $\psi : S \to T$.

Lause 1.2.1. *Olgu $\varphi : S \to T$ homomorfism. Siis hulk $S\varphi \subseteq T$ on alampoolrühm.*

Tõestus. Piisab näidata, et hulk $S\varphi$ on kinnine korrutamise suhtes. Kuna φ on homomorfism, siis mistahes elementide $s, s' \in S$ korral

$$ss' \in S \quad \text{ja} \quad (s\varphi)(s'\varphi) = (ss')\varphi \in S\varphi.$$

Järelikult $S\varphi$ on poolrühma T alampoolrühm. ■

Kui S, T on monoidid, siis $\varphi : S \to T$ on **monoidide homomorfism**, kui φ on poolrühmade homomorfism, mille korral $1_S \mapsto 1_T$.

Definitsioon. Olgu $\varphi : S \to T$ poolrühmade homomorfism, siis φ **tuumaks** nimetatakse seost $\ker\varphi \subseteq S \times S$, mis on defineeritud järgmiselt:

$$x \ker\varphi\, y \iff x\varphi = y\varphi \qquad (x, y \in S).$$

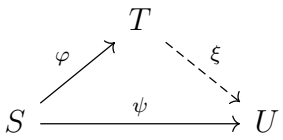
Teame, et võrdsusseos '=' on ekvivalentsiseos. Edaspidi, tähistame võrdsusseost kui hulka sümboliga $\mathscr{E}$. Lihtne on veenduda, et $\ker\varphi$ on kongruents poolrühmal S, kusjuures φ on injektiivne parajasti siis, kui $\ker\varphi = \mathscr{E}$.

Kui ρ on seos mingil mittetühjal hulgal A, siis võime seda seost ahendada mistahes alamhulgale $B \subseteq A$, tähistades $\rho|_B$, kusjuures

$$\rho|_B := \rho \cap (B \times B) = \{(b, b') \in B \times B : b\rho b'\}.$$

Lihtne on veenduda asjaolus, et kui $S' \subseteq S$ on alampoolrühm ja $\varphi : S \to T$ on poolrühmade homomorfism, siis ka $\varphi|_{S'} : S' \to T$ on poolrühmade homomorfism.

Lause 1.2.2 ([G] I.3.5). *Olgu T, U poolrühmad. Olgu $\varphi : S \to T$ sürjektiivne homomorfism ja $\psi : S \to U$ homomorfism. Siis $\ker\varphi \subseteq \ker\psi$ parajasti siis, kui leidub üheselt määratud homomorfism $\xi : T \to U$ nii, et $\psi = \varphi\xi$ (öeldakse ka, et ψ on φ-kordne).*



Tõestus. Leidugu homomorfism $\xi : T \to U$ nii, et $\psi = \varphi\xi$. Siis iga $x, y \in S$ korral

$$x \ker\varphi y \Longrightarrow x\varphi = y\varphi \Longrightarrow x\psi = (x\varphi)\xi = (y\varphi)\xi = y\psi,$$

järelikult $x \ker\psi y$, seega $\ker\varphi \subseteq \ker\psi$.

Olgu nüüd $\ker\varphi \subseteq \ker\psi$. Kuna φ on sürjektiivne, siis iga $t \in T$ korral leidub $s \in S$ nii, et $t = s\varphi$. Defineerime kujutuse

$$\xi : T \to U, \quad s\varphi \mapsto s\psi.$$

Kui leiduvad $s', s'' \in S$ nii, et elemendile $t \in T$ seatakse vastavusse $s'\psi$ ja $s''\psi$, siis eelduse $\ker\varphi \subseteq \ker\psi$ tõttu

$$t = s'\varphi = s''\varphi \Longrightarrow s' \ker\varphi s'' \Longrightarrow s' \ker\psi s'',$$

järelikult $s'\psi = s''\psi$, millega oleme näidanud, et kujutus ξ on korrektselt defineeritud.

Olgu $x\varphi, y\varphi \in T$. Kuna φ ja ψ on homomorfismid, siis

$$((x\varphi)(y\varphi))\xi = (xy)\varphi\xi = (xy)\psi = (x\psi)(y\psi) = (x\varphi)\xi\,(y\varphi)\xi,$$

seega ξ on homomorfism. Kui $\xi' : T \to U$ nii, et $\psi = \varphi\xi'$ ja $x\varphi \in T$, siis

$$(x\varphi)\xi = x\psi = (x\varphi)\xi',$$

seega $\xi = \xi'$. ■

Toome sisse ka mõned mõisted rühmateooriast.

Olgu G, H rühmad, siis $\varphi : G \to H$ on **rühmade homomorfism**, kui φ on monoidide homomorfism.

Definitsioon. Olgu G rühm ja $H \subseteq G$ alamrühm. Öeldakse, et H on **normaalne alamrühm** ($H \trianglelefteq G$) rühmas G, kui iga $g \in G$ korral $gH = Hg$. Tähistatakse $H \triangleleft G$, kui $H \subset G$ on normaalne pärisalamrühm.

Lihtne on mõista, et 1 ja G on rühma G normaalsed alamrühmad, neile viidatakse kui

triviaalsetele normaalsetele alamrühmadele. Öeldakse, et rühm G on **lihtne**, kui ta ei sisalda mittetriviaalseid normaalseid alamrühmi.

Õpikus [K1] näidatakse, et saadakse klassijaotus rühma normaalse alamrühma abil järgmiselt:

$$G/H := \{gH : g \in G\},$$

kusjuures hulk G/H on rühm korrutamise suhtes, mis on defineeritud esindajate kaudu ehk mistahes $f, g \in G$ korral

$$(fH)(gH) := (fg)H.$$

Lemma 1.2.3 ([K1] VI.1.10). *Olgu G rühm ja $H \subseteq G$ alamrühm. Siis iga $f, g \in G$ korral*

$$fH = gH \iff g^{-1}f \in H.$$

Järgnev lõik põhineb õpikul [K2].
Kui rühmal G leidub konstruktsioon

$$1 =: G_0 \lhd G_1 \lhd \ldots \lhd G_{k-1} \lhd G_k := G \qquad (k \in \mathbb{N}),$$

siis öeldakse, et see on rühma G **normaaljada**. Maksimaalse pikkusega normaaljada nimetatakse rühma G **kompositsioonijadaks**. Teada on, et igal lõplikul rühmal eksisteerib kompositsioonijada. Näidatakse, et kompositsioonijadas iga rühm $G_j/G_{j-1}, j = 1, \ldots, k$, ehk kompositsioonijada faktor, on lihtne rühm.

Grillet' monograafia [G] põhjal osutub oluliseks mõisteks ka järgmine.

Definitsioon. Rühm G on rühma N **laiendrühm rühma** Q **abil**, kui $N \trianglelefteq G$ ja $Q \cong G/N$.

1.3 Rees'i kongruents ja otsekorrutised

Olgu $I \subseteq S$ ideaal poolrühmas S. Defineeritakse seos $\mathscr{F} \subseteq S \times S$ järgmiselt:

$$a \mathscr{F} b \iff (a = b \quad \text{või} \quad a, b \in I) \qquad (a, b \in S).$$

Näidatakse, et tegemist on kongruentsiga poolrühmal S (vt [G] I.4.6), mida nimetatakse ideaali $I \subseteq S$ poolt tekitatud **Rees'i kongruentsiks**, kusjuures poolrühm $S/I := S/\mathscr{F}$ samastatakse hulgaga $(S \setminus I) \cup \{0\}$ ning defineeritakse korrutamine $*$ järgmiselt:

$$x * y = \begin{cases} xy, & xy \in S \setminus I \\ 0, & xy \in I \end{cases} \qquad (x, y \in S \setminus I).$$

Saadud poolrühma nimetatakse ideaali I **Rees'i faktorpoolrühmaks**.

Olgu Q nulliga poolrühm nii, et $Q \cap S = \emptyset$. Poolrühma S **Cliffordi laiendiks** nulliga poolrühma Q **abil** nimetame poolrühma E, mille korral $S \subseteq E$ on ideaal ja $Q \cong {}^{E}\!/_{S}$ (vt [G] III.1). Kui kontekstist on nulliga poolrühma Q roll üheselt mõistetav, siis ütleme lühidalt, et E on poolrühma S Cliffordi laiend.

Homomorfismi $\eta : S \to S$, mille korral η on idempotentne teisendus ehk $\eta^2 = \eta$, nimetatakse **retraktsiooniks**.

Standardne tulemus algebras on poolrühmade homomorfismiteoreem, millega analoogiline rühmateoreetiline väide on esitatud õpikus [K2] (vt II.1.2).

Teoreem. *Olgu $\varphi : S \to T$ poolrühmade homomorfism. Siis leidub injektiivne poolrühmade homomorfism $\psi : {}^{S}\!/_{\ker\varphi} \to T$ nii, et $\varphi = \pi\psi$, kus $\pi : S \to {}^{S}\!/_{\ker\varphi}$ on loomulik projektsioon.*

Lause 1.3.1 ([G] III.1.8). *Olgu E poolrühma S Cliffordi laiend. Kui leidub retraktsioon η poolrühmal E, mille korral $E\eta = S$, siis leidub kongruents $\mathscr{C}$ poolrühmal E, mille korral $\mathscr{C}|_S = \mathscr{E}$ ja ${}^{E}\!/_{\mathscr{C}} \cong S$.*

Tõestus. Olgu $\eta : E \to E$ retraktsioon, mille korral $E\eta = S$. Paneme tähele, et $\ker\eta|_S = \mathscr{E}$. Triviaalselt kehtib $\mathscr{E} \subseteq \ker\eta|_S$. Teisalt, olgu $s, t \in S$, mille korral $s \ker\eta\, t$ ehk $s\eta = t\eta$. Kuna $E\eta = S$, siis leiduvad $u, v \in S$ nii, et $u\eta = s$ ja $v\eta = t$. Et η on idempotent, siis

$$s = u\eta = s\eta = t\eta = v\eta = t,$$

seega $\ker\eta|_S = \mathscr{E}$. Homomorfismiteoreemi põhjal ${}^{E}\!/_{\ker\eta} \cong E\eta = S$. ■

Olgu A mingi hulk ja $(S_\alpha)_{\alpha\in A}$ poolrühmad. Poolrühmade S_α **otsekorrutiseks** nimetatakse poolrühma

$$P := \prod_{\alpha\in A} S_\alpha = \{(s_\alpha)_{\alpha\in A} : \alpha \in A, s_\alpha \in S_\alpha\},$$

kus korrutamine on defineeritud komponenthaaval ehk

$$(s_\alpha)_{\alpha\in A}(t_\alpha)_{\alpha\in A} = (s_\alpha t_\alpha)_{\alpha\in A} \qquad (s_\alpha, t_\alpha \in S_\alpha, \alpha \in A).$$

Osutub, et selline korrutamine on ainus selline, et iga $\alpha \in A$ korral projektsioonid

$$\pi_\alpha : P \to S_\alpha, (x_\alpha)_{\alpha\in A} \mapsto x_\alpha$$

on homomorfismid. Poolrühmade $S_\alpha, \alpha \in A$ **alamotsekorrutiseks** nimetatakse alampoolrühma $T \subseteq P$ nii, et iga $\alpha \in A$ korral $T\pi_\alpha = S_\alpha$. Mistahes poolrühma kohta,

mis on isomorfne mingi sellise alampoolrühmaga T, öeldakse, et see on poolrühma P alamotsekorrutis.

Olgu $T \subseteq P$ alamotsekorrutis ja $p_\alpha : T \to S_\alpha, \alpha \in A$ homomorfismid. Öeldakse, et homomorfismide kogum $p_\alpha, \alpha \in A$ **eraldab** poolrühma T elemendid, kui kehtib implikatsioon

$$(\forall \alpha \in A)\,(xp_\alpha = yp_\alpha) \Longrightarrow x = y. \tag{1}$$

Lause 1.3.2 ([G] III.3.1). *Järgmised väited on samaväärsed.*

(a) S on poolrühmade $S_\alpha, \alpha \in A$ alamotsekorrutis.

(b) Leidub sürjektiivsete homomorfismide kogum $S \to S_\alpha, \alpha \in A$, mis eraldab poolrühma S elemendid.

Tõestus. Lihtne on mõista, et väide (b) on piisav väite (a) kehtivuseks.

Kehtigu väide (a). Tähistagu P poolrühmade $S_\alpha, \alpha \in A$ otsekorrutist. Leidub alampoolrühm $T \subseteq P$ nii, et $S \cong T$ ja iga $\alpha \in A$ korral $T\pi_\alpha = S_\alpha$. Samastame poolrühmad S ja T ning iga $\alpha \in A$ korral ahendame projektsiooni $\pi_\alpha|_S =: p_\alpha$, siis on selge, et tegemist on sürjektiivse homomorfismiga. Näitame, et kehtib implikatsioon (1). Olgu $x, y \in S$ nii, et iga $\alpha \in A$ korral $xp_\alpha = yp_\alpha$, siis elementide x, y vastavad komponendid on võrdsed, järelikult $x = y$. ■

Lause 1.3.3 ([G] III.3.2). *Olgu $\mathscr{C}_\alpha, \alpha \in A$ kongruentsid poolrühmal S ja $\mathscr{C} = \bigcap_{\alpha\in A} \mathscr{C}_\alpha$ kongruents poolrühmal S. Siis poolrühm $S/\mathscr{C}$ on poolrühmade $S/\mathscr{C}_\alpha, \alpha \in A$ alamotsekorrutis.*

Tõestus. Olgu kujutused

$$\pi : S \to S/\mathscr{C} \quad \text{ja} \quad \pi_\alpha : S \to S/\mathscr{C}_\alpha, \alpha \in A$$

loomulikud projektsioonid. Kuna iga $\alpha \in A$ korral $\mathscr{C} \subseteq \mathscr{C}_\alpha$, siis iga α korral leidub üheselt määratud homomorfism $\sigma_\alpha : S/\mathscr{C} \to S/\mathscr{C}_\alpha$ nii, et $\pi_\alpha = \pi\sigma_\alpha$ (vt lause 1.2.2). Lihtne on mõista, et iga $\alpha \in A$ korral kujutus σ_α on sürjektiivne homomorfism. Paneme tähele, et homomorfismide kogum $\sigma_\alpha, \alpha \in A$ eraldab poolrühma $S/\mathscr{C}$ elemendid. Tõepoolest, olgu $[a], [b] \in S/\mathscr{C}$ sellised, et iga $\alpha \in A$ korral $[a]\sigma_\alpha = [b]\sigma_\alpha$. Kuna iga $a \in S$ korral $a\pi = [a]$, siis

$$(\forall \alpha \in A)\,((a\pi)\sigma_\alpha = (b\pi)\sigma_\alpha)\,.$$

Seega iga $\alpha \in A$ korral $a\pi_\alpha = b\pi_\alpha$ ehk $a\mathscr{C}_\alpha b$, seega $a\mathscr{C}b$ ja $[a] = [b]$. Lause 1.3.2 põhjal poolrühm $S/\mathscr{C}$ on poolrühmade $S/\mathscr{C}_\alpha, \alpha \in A$ alamotsekorrutis. ■

1.4 Lõplikud poolrühmad

Käesolevas paragrahvis olgu S lõplik poolrühm.

Definitsioon. Poolrühma T nimetatakse **monogeenseks**, kui leidub $x \in T$ nii, et $T = \{x^n : n \in \mathbb{N}\}$. Sel juhul elementi x nimetatakse poolrühma T **moodustajaks**. Kui x on poolrühma T moodustaja, siis tähistatakse $T = \langle x \rangle$.

Lihtne on mõista, et poolrühma T mistahes elemendi poolt moodustatud alamhulk on alampoolrühm.

Lause 1.4.1. *Iga elemendi $x \in S$ korral leidub $m \in \mathbb{N}$ nii, et x^m on idempotent.*

Tõestus. Fikseerime vabalt $x \in S$ ning vaatleme hulka

$$\left\{x^{2^t} : t \in \mathbb{N} \cup \{0\}\right\} \subseteq S.$$

Kuna S on lõplik, siis leiduvad $r, s \in \mathbb{N} \cup \{0\}$ nii, et $x^{2^r} = x^{2^s}$ ja $r \neq s$. Olgu üldisust kitsendamata $r > s$ ehk $r = s + u$, kus $u \in \mathbb{N}$. Tähistame $z := x^{2^s}$, siis $z = z^{2^u}$. Paneme tähele, et

$$\left(z^{2^u-1}\right)^2 = z^{2(2^u-1)} = z^{2^u} \cdot z^{2^u-2} = z \cdot z^{2^u-2} = z^{2^u-1}$$

ehk z^{2^u-1} on idempotent. ■

Lemma 1.4.2 ([G] V.1.1). *Mistahes elementide $x \in S$ ja $u, v \in S^1$ korral kehtib implikatsioon*

$$uxv \mathscr{J} x \Longrightarrow ux\mathscr{L}x\mathscr{R}xv.$$

Tõestus. Olgu $w, z \in S^1$ omadusega $w(uxv)z = x$. Kui mingi $n \in \mathbb{N}$ korral $(wu)^n x(vz)^n = x$, siis märgime, et

$$(wu)^{n+1}x(vz)^{n+1} = wu(wu)^n x(vz)^n vz = wuxvz = x.$$

Olgu lause 1.4.1 põhjal $m \in \mathbb{N}$ selline, et $(wu)^m =: f \in S^1$ on idempotent, siis

$$fx = (wu)^m(wu)^m x(vz)^m = (wu)^m x(vz)^m = x,$$

kusjuures $x \leq_{\mathscr{L}} ux \leq_{\mathscr{L}} (wu)^m x = x$, seega $ux\mathscr{L}x$. Analoogiliselt, olgu $r \in \mathbb{N}$ nii, et $(vz)^r =: g$ on idempotent, siis $xg = x$ ning $x = x(vu)^r \leq_{\mathscr{R}} xv \leq_{\mathscr{R}} x$ ehk $x\mathscr{R}xv$. ■

Lause 1.4.3 ([G] V.1.2). *Olgu T poolrühm, siis $\mathscr{D} \subseteq \mathscr{J}$. Igas lõplikus poolrühmas $\mathscr{D} = \mathscr{J}$.*

Tõestus. Näitame kõigepealt, et suvalises poolrühmas $\mathscr{D} \subseteq \mathscr{J}$. Selleks, olgu $x, y \in T$ ja $x \mathscr{D} y$ ehk leidub $z \in T$ nii, et $x \mathscr{L} z \mathscr{R} y$. Seoste $\mathscr{L}$ ja $\mathscr{R}$ kirjelduste põhjal leiduvad $u, v \in T^1$ omadusega $x = uz$ ja $z = yv$, järelikult $x = uyv$ ehk $x \leq_{\mathscr{J}} y$. Teisalt, leiduvad $s, t \in T^1$ nii, et $y = zs$ ja $z = tx$, seega $y = txs$ ehk $y \leq_{\mathscr{J}} x$. Kokkuvõttes, oleme näidanud, et $x \mathscr{J} y$.

Olgu nüüd T lõplik poolrühm ja veendume, et $\mathscr{J} \subseteq \mathscr{D}$. Selleks, olgu $x, y \in T$ ja $x \mathscr{J} y$. Leiduvad $u, v \in T^1$ nii, et $y = uxv$ ning lemma 1.4.2 põhjal kehtib $x \mathscr{R} xv$. Kuna $u(xv)1 \mathscr{J} xv$, siis ka $xv \mathscr{L} uxv$. Kokku oleme saanud, et $uxv \mathscr{L} xv \mathscr{R} x$ ehk $y \mathscr{D} x$. Et seos $\mathscr{D}$ on sümmeetriline, siis $x \mathscr{D} y$. ■

Grillet' monograafia [G] põhjal toome sisse järgmise mõiste. **Bitsükliliseks poolrühmaks** nimetatakse kahest moodustajast p, q moodustatud monoidi, mis defineeritakse $C := \langle p, q; pq = 1 \rangle$. Näidatakse, et iga element hulgas C esitub üheselt kujul $q^m p^n$, kus $m, n \in \mathbb{N}$ (vt [G] I.6.3), millest on vahetu järeldada, et iga bitsükliline poolrühm on lõpmatu hulk.

Tuuakse ka välja, et kui $\mathscr{C}$ on kongruents bitsüklilisel poolrühmal ja $\mathscr{C}$ ei ole võrdsusseos, siis $qp \mathscr{C} 1$ (vt [G] I.6.4).

Lause 1.4.4 ([G] II.2.7). *Olgu S poolrühm ja J poolrühma S $\mathscr{J}$-klass. Kui hulk J sisaldab idempotendid $f < e$, siis J sisaldab bitsüklilise poolrühma.*

Tõestus. Olgu $e \mathscr{J} f$, siis leiduvad $u, v \in S^1$ omadusega $e = ufv$. Lihtne on veenduda, et elementide

$$a := euf \quad \text{ja} \quad b := fve$$

korral $ea = a = ae$ ja $eb = b = be$, kusjuures

$$ab = eaeb = eeb = eb = e,$$

järelikult $a, b \in J$ ning paneme tähele, et $ba = (fve)(euf) = fveuf \leq f$. Kuna $f < e$, siis $ba \neq e$ ja hulk $T = \langle a, b \rangle$ on monoid ühikelemendiga e. Olgu $C = \langle p, q; pq = 1 \rangle$ bitsükliline poolrühm. Defineerime kujutuse

$$\varphi : C \to T, \quad p \mapsto a \quad \text{ja} \quad q \mapsto b.$$

Lihtne on mõista, et tegemist on sürjektiivse homomorfismiga. Veelgi enam, kuna $ba \neq e$, siis kongruents $\mathscr{C} := \ker\varphi$ ei rahulda tingimust $qp \mathscr{C} 1$, seega φ on isomorfism ja T on bitsükliline poolrühm. Olgu $x, y \in C$ ning olgu $x = q^m p^n$ ja $y = q^r p^s, m, n, r, s \in \mathbb{N}$,

siis lihtne on mõista, et

$$q^m p^n \mathscr{L} q^r p^n \mathscr{R} q^r p^s,$$

seega $x \mathscr{D} y$ ja lause 1.4.3 põhjal $T \subseteq J$. ■

Lause 1.4.5 ([G] V.1.3). *Olgu S lõplik monoid. Siis $H_1 = L_1 = R_1 = J_1$ ja hulk $S \setminus J_1$ on ideaal monoidis S.*

Tõestus. Triviaalselt kehtib $H_1 \subseteq L_1$. Olgu $x \in L_1$, siis leidub $y \in S$ nii, et $yx = 1$, kusjuures

$$(xy)^2 = (xy)(xy) = x(yx)y = x1y = xy$$

ehk xy on idempotent. Kuna 1 on idempotent ja J_1 on lõplik hulk, siis lause 1.4.4 põhjal $xy < 1$ on võimatu, seega $xy = 1$ ja $x \in H_1$. Analoogiliselt näidatakse, et $R_1 = H_1$, järelikult D_1 koosneb täpselt ühest $\mathscr{L}$-klassist ja täpselt ühest $\mathscr{R}$-klassist. Kuna S on lõplik, siis lause 1.4.3 põhjal $J_1 = D_1 = H_1$. Paneme tähele, et $S \setminus J_1$ esitub kujul

$$S \setminus J_1 = \bigcup_{J < J_1} J.$$

Tõepoolest, kui $x \in S \setminus J_1$, siis leidub $\mathscr{J}$-klass $J := J_a$, mis sisaldab x. Kuna $a \neq 1$ ja $a = a11$, siis $a \leq_{\mathscr{J}} 1$, järelikult $J_a < J_1$. Teistpidi sisalduvus on ilmne. Et iga $\mathscr{J}$-klass on ideaal ja ideaalide ühend on samuti ideaal, siis ka $S \setminus J_1$ on ideaal. ■

Poolrühmade jaguvus ja põimikkorrutis

Käesolev peatükk põhineb paragrahvil V.3 Grillet' monograafiast [G].

2.1 Poolrühmade jaguvus

Definitsioon. Öeldakse, et poolrühm S **jagab** poolrühma T, tähistatakse $S \prec T$, kui leidub alampoolrühm $T' \subseteq T$ ja sürjektiivne homomorfism $\varphi : T' \to S$.

Lause 2.1.1. *Kehtivad järgmised väited.*

(a) Olgu $S' \subseteq S$ alampoolrühm. Siis $S' \prec S$.

(b) Olgu T poolrühm ja $\varphi : S \to T$ injektiivne homomorfism. Siis $S \prec T$.

Tõestus. Märgime (a) osa tõestuseks, et kujutus

$$\mathrm{id}_{S'} : S' \to S', \quad s \mapsto s$$

on sürjektiivne homomorfism, järelikult $S' \prec S$.

Olgu $\varphi : S \to T$ injektiivne homomorfism, siis lause 1.2.1 põhjal $S\varphi \subseteq T$ on alampoolrühm, kusjuures $S \cong S\varphi$, seega leidub φ^{-1}, mis on samuti isomorfism. ■

Lause 2.1.2 ([G] V.3). *Poolrühmade jaguvusseos on transitiivne.*

Tõestus. Olgu T, U poolrühmad ja kehtigu $S \prec T \prec U$ ehk leiduvad alampoolrühmad $U' \subseteq U$ ja $T' \subseteq T$ ning sürjektiivsed homomorfismid $\psi : U' \to T$ ja $\varphi : T' \to S$. Näitame, et $S \prec U$, milleks piisab leida alampoolrühm $V \subseteq U$ ja sürjektiivne homomorfism $\xi : V \to S$.

Paneme tähele, et hulk

$$V := \psi^{-1}(T') = \{v \in U' : v\psi \in T'\} \subseteq U'$$

on alampoolrühm. Tõepoolest, olgu $u, v \in V$, siis $u\psi, v\psi \in T'$. Kuna $T' \subseteq T$ on alampoolrühm ja ψ on homomorfism, siis

$$(uv)\psi = (u\psi)(v\psi) \in T',$$

järelikult $uv \in V$. Kuna ψ on sürjektiivne, siis ka $\psi|_V : V \to T'$ on sürjektiivne. Selleks märgime, et kui $t \in T'$, siis leidub $v \in U'$ omadusega $v\psi = t \in T'$. Konstruktsiooni põhjal $v \in V$, kusjuures nüüd

$$(V\psi|_V)\,\varphi = T'\varphi = S,$$

seega $\psi|_V\varphi : V \to S$ on sürjektiivne homomorfism. ■

Edaspidi tihti kasutame lause 2.1.2 väidet, millele lühidalt viitame kui transitiivsusele.

Kui poolrühma T korral kehtib $S \prec T$, siis öeldakse ka, et S on poolrühma T mingi alampoolrühma **homomorfne kujutis**.

2.2 Poolrühmade põimikkorrutis

Olgu A poolrühm. Lihtne on veenduda, et hulk $A^S = \{f : S \to A\}$ on poolrühm punktiviisiliselt defineeritud korrutamise suhtes:

$$x(fg) = (xf)(xg)$$

mistahes $f, g \in A^S,\ x \in S$ korral. Me loodame, et punktiviisiline korrutamine ei lähe segi kujutuste järjestrakendamisega. Selguse huvides kujutusi tähistame ladina tähtede $f, g, h, \ldots$ abil ja homomorfisme kreeka tähtede $\varphi, \psi, \xi, \ldots$ abil.

Kui $g : S \to A$ ja $s \in S$, siis defineerime kujutuse ${}^s g : S \to A$ nii, et iga $s \in S$ korral

$$x\ {}^s g = (xs)g.$$

Hulgal $A^S \times S$ defineeritakse korrutamine nii, et iga $f, g \in A^S$ ja iga $s, t \in S$ korral

$$(f, s) * (g, t) := (f\ {}^s g, st)\,,$$

kus $f\ {}^s g$ on kujutuste f ja ${}^s g$ punktiviisiline korrutis ehk iga $s \in S$ korral

$$x\,(f\ {}^s g) = (xf)(xs)g.$$

Paneme tähele, et iga $x \in S$ korral

$$x\ {}^{s}(fg) = (xs)(fg) = (xs)f\,(xs)g = (x\ {}^{s}f)\,(x\ {}^{s}g) = x\,(\ {}^{s}f\ {}^{s}g)\,,$$

seega ${}^{s}(fg) = (x)\ {}^{s}f\,(x)\ {}^{s}g = x\ {}^{s}f\,(x\ {}^{s}g = {}^{s}f\ {}^{s}g$. Osutub, et korrutamine $*$ on assotsiatiivne. Tõepoolest, olgu $h \in A^S$ ja $u \in S$, siis

$$\begin{aligned}
&[(f,s)*(g,t)]*(h,u) = (f\ {}^{s}g, st)*(h,u) = \\
&\left(f\ {}^{s}g\ {}^{st}h, stu\right) = \left(f\ {}^{s}\left(g\ {}^{t}h\right), stu\right) = (f,s)*\left(g\ {}^{t}h, tu\right) = \\
&(f,s)*[(g,t)*(h,u)],
\end{aligned}$$

millega oleme näidanud, et paar $(A^S \times S, *)$ on poolrühm.

Definitsioon. Poolrühma $(A^S \times S, *)$ nimetatakse poolrühmade A ja S **põimikkorrutiseks** ja tähistatakse $A \wr S$.

Edaspidi me kirjas ei erista korrutamistehet $*$ kuna tema roll on kontekstist üheselt mõistetav.

Olgu A ja S monoidid, mille ühikelemente tähistame sümboliga 1. Vaatleme konstantset kujutust

$$e : S \to A, \quad x \mapsto 1.$$

Osutub, et poolrühm $A \wr S$ on samuti monoid ühikelemendiga $(e,1)$. Tõepoolest, olgu $(f,s) \in A \wr S$, siis

$$(f,s)(e,1) = (f\ {}^{s}e, s1) = (f,s) \quad \text{ja} \quad (e,1)(f,s) = (e\ {}^{1}f, 1s) = (f,s),$$

sest iga $x \in S$ korral kehtivad

$$x\,(f\ {}^{s}e) = (xf)(xs)e = (xf)1 = xf \quad \text{ja} \quad x\left(e\ {}^{1}f\right) = (xe)(x1)f = 1(xf) = xf.$$

Lause 2.2.1 ([G] V.3). *Olgu $A = \{a\}$ triviaalne poolrühm. Siis iga poolrühma S korral $A \wr S \cong S$.*

Tõestus. Kui $f \in A^S$, siis iga $s \in S$ korral $sf = a$, mistõttu kujutus

$$\varphi : A \wr S \to S, \quad (f,s) \mapsto s$$

on isomorfism. ■

Kui A ja S on lõplikud poolrühmad, milles on vastavalt $m, n \in \mathbb{N}$ elementi, siis hulk $A \wr S$ sisaldab $m^n n$ elementi. Kui poolrühmas T on $r \in \mathbb{N}$ elementi, siis hulk

$(A \wr S) \wr T$ sisaldab $(m^n n)^r r$ elementi, kuid hulk $A \wr (S \wr T)$ sisaldab $m^{n^r r} n^r r$ elementi, järelikult põimikkorrutamine üldiselt ei ole assotsiatiivne. Kokkuleppeliselt loetakse, et

$$A \wr B \wr C := (A \wr B) \wr C.$$

Lause 2.2.2 ([G] V.3.1). *Olgu G rühma N laiendrühm rühma Q abil. Siis leidub alampoolrühm $T \subseteq N \wr Q$ nii, et $G \cong T$, muuhulgas $G \prec N \wr Q$.*

Tõestus. Olgu $N \trianglelefteq G$ ja $Q \cong {}^{G}\!/_{N}$, kusjuures olgu isomorfismi realiseeriv kujutus

$$\tau : {}^{G}\!/_{N} \to Q$$

ja olgu

$$\pi : G \to {}^{G}\!/_{N} \quad g \mapsto gN$$

loomulik projektsioon. Tähistame $\pi\tau =: \hat{\pi}$, siis $\hat{\pi} : G \to Q$ on sürjektiivne rühmade homomorfism. Fikseerime iga $s \in Q$ jaoks ühe sellise elemendi $p_s \in G$ omadusega $s = p_s\hat{\pi}$. Võime võtta $p_1 = 1$ kuna $\hat{\pi}$ on rühmade homomorfism. Näitame, et

$$(\forall g \in G)\,(\exists s \in Q)\,(\exists! a \in N)\,(g = ap_s)\,,$$

kus $s = g\hat{\pi}$. Olgu $g \in G$ ja $s = g\hat{\pi} \in Q$, siis

$$g\hat{\pi} = p_{g\hat{\pi}}\hat{\pi} \Longrightarrow (p_s N)\tau = (gN)\tau \Longrightarrow p_s N = gN.$$

Kuna $N \trianglelefteq G$, siis $Np_s = gN$, järelikult leidub $a \in N$ omadusega $g = ap_s$. Kui leidub $b \in N$ omadusega $ap_s = bp_s$, siis $a = b$, seega $a \in N$ on üheselt määratud. Eelneva põhjal, iga $u \in Q$ ja iga $g \in G$ korral

$$p_u g = a p_{(p_u g)\hat{\pi}} = a p_{u(g\hat{\pi})},$$

kus $a \in N$ on üheselt määratud. Olgu $u \in Q$ ja $g \in G$. Oleme näidanud, et

$$(\exists! a \in N)(p_u g = a p_{us}),$$

kus $s = g\hat{\pi}$. Defineerime kujutuse $\overline{g} : Q \to N$, kus loeme $u\overline{g} := a$. Defineerime nüüd kujutuse

$$\psi : G \to N \wr Q, \quad g \mapsto (\overline{g}, g\hat{\pi}).$$

Näitame, et ψ on injektiivne. Olgu mingi $g, h \in G$ korral $g\psi = h\psi$, siis $g\hat{\pi} = h\hat{\pi} = s$ ja

$$g = 1g = p_1 g = (1\overline{g})p_s = (1\overline{h})p_s = p_1 h = 1h = h,$$

seega ψ on injektiivne. Näitame veel, et ψ on homomorfism. Kui $g\hat{\pi} = s$ ja $h\hat{\pi} = t$,

siis $(g\psi)(h\psi) = (\overline{g}, s)(\overline{h}, t) = (\overline{gh}, st)$, sest iga $u \in Q$ korral

$$u\left(\overline{g}\ {}^{\overline{s}}\overline{h}\right) p_{ust} = (u\overline{g})(us)\overline{h}p_{ust} = (u\overline{g})p_{us}h = p_u gh = (u\overline{gh})p_{ust},$$

järelikult ψ on homomorfism, muuhulgas lause 2.1.1 (b) osa põhjal $G \prec N \wr Q$. ■

Tõestame veel mõned põimikkorrutise omadused.

Lause 2.2.3 ([G] V.3.2). *Olgu A poolrühm. Siis kehtivad järgmised väited.*

(a) $A \prec A \wr S$,

(b) $S \prec A \wr S$,

(c) $A \times S \prec A \wr S$.

Tõestus. Hulk $A \times S$ on poolrühm korrutamise

$$(a, s)(b, t) = (ab, st) \qquad (a, b \in A, \quad s, t \in S)$$

suhtes. Projektsioonid

$$A \times S \to A, \quad (a, s) \mapsto a \quad \text{ja} \quad A \times S \to S, \quad (a, s) \mapsto s$$

on sürjektiivsed homomorfismid, järelikult $A \prec A \times S$ ja $S \prec A \times S$.
Näitame, et $A \times S \prec A \wr S$. Defineerime iga $a \in A$ korral kujutuse

$$c_a : S \to A, \quad s \mapsto a.$$

Siis hulk $T := \{(c_a, s) : a \in A, s \in S\} \subset A \wr S$ on alampoolrühm. Tõepoolest, olgu $a, b \in A$ ja $s, t \in S$. Kuna iga $x \in S$ korral

$$x\,(c_a\ {}^{s}c_b) = (xc_a)(xs)c_b = ab,$$

siis $(c_a, s)(c_b, t) = (c_{ab}, st) \in T$. Defineerime kujutuse

$$\omega : T \to A \times S, \quad (c_a, s) \mapsto (a, s),$$

siis iga $a, b \in A$ ja $s, t \in S$ korral

$$(c_{ab}, st)\,\omega = (ab, st) = (a, s)(b, t) = (c_a, s)\,\omega\ (c_b, t)\,\omega,$$

seega ω on isomorfism ja $A \times S \prec A \wr S$. Transitiivsuse põhjal $A \prec A \wr S$ ja $S \prec A \wr S$. ■

Lause 2.2.4 ([G] V.3.4). *Poolrühmade jaguvusseos on kooskõlas põimikkorrutamisega ehk mistahes poolrühmade A, B, T korral*

$$A \prec B \quad \textit{ja} \quad S \prec T \Longrightarrow A \,\mathsf{w}\, S \prec B \,\mathsf{w}\, T.$$

Tõestus. Tõestame kõigepealt kaks erijuhtu.

(a) Hulgad $A \subseteq B$ ja $S \subseteq T$ on alampoolrühmad.

(b) Hulgad A ja S on vastavalt poolrühmade B ja T homomorfsed kujutised.

Tõestame (a) osa. Olgu $A \subseteq B$ ja $S \subseteq T$ alampoolrühmad. Tähistame

$$V := \{(f,t) \in B \,\mathsf{w}\, T : t \in S, Sf \subseteq A\} \subseteq B \,\mathsf{w}\, T.$$

Kui $(f,t),(g,u) \in V$, siis $(f,t)(g,u) = (f\ {}^t g, tu)$, kus $tu \in S$ ja iga $x \in S$ korral

$$x\left(f\ {}^t g\right) = (xf)(xt)g \in A,$$

järelikult V on alampoolrühm. Defineerime kujutuse

$$\varphi : V \to A \,\mathsf{w}\, S, \quad (f,t) \mapsto (f|_S, t),$$

kus $f|_S : S \to A$ ning veendume, et tegemist on homomorfismiga. Selleks olgu $(f,t),(g,u) \in V$, siis

$$((f,t)(g,u))\,\varphi = \left((f\ {}^t g, tu)\right)\varphi = \left((f\ {}^t g)|_S, tu\right) = (f|_S, t)\,(g|_S, u) = (f,t)\varphi\,(g,u)\varphi.$$

Tõepoolest, tähistame $(h, tu) := (f|_S, t)\,(g|_S, u)$ ehk iga $x \in S$ korral $xh = (xf|_S)(xt)g|_S$. Siis iga $x \in S$ korral

$$x\left(f\ {}^t g\right)|_S = (xf)(xt)g = (xf|_S)(xt)g|_S = xh.$$

Kui $(g,t) \in A \,\mathsf{w}\, S$, siis valime $f \in B^T$ nii, et $f|_S = g$, millest $(f|_S, t)\varphi = (g,t)$, seega φ on sürjektiivne, millega oleme näidanud, et $A \,\mathsf{w}\, S \prec B \,\mathsf{w}\, T$.

Tõestame (b) osa. Olgu $\varphi : B \to A$ ja $\psi : T \to S$ sürjektiivsed homomorfismid. Kuna ψ on sürjektiivne, siis iga $f \in B^T$ korral $f\varphi$ on ψ-kordne parajasti siis, kui kehtib implikatsioon

$$x\psi = y\psi \Longrightarrow (xf)\varphi = (yf)\varphi \qquad (x, y \in T). \tag{2}$$

Tõepoolest, kui leidub $g : S \to A$ nii, et $f\varphi = \psi g$, siis iga $x, y \in T$ korral

$$x\psi = y\psi \Longrightarrow (x\psi)g = (y\psi)g \iff (xf)\varphi = (yf)\varphi.$$

Teisalt, kehtigu implikatsioon (2). Defineerime

$$g : S \to A, \quad s \mapsto t(f\varphi),$$

kus $t \in T$ on omadusega $t\psi = s$. Olgu $s \in S$ ja $t, t' \in T$ nii, et $t\psi = t'\psi = s$. Implikatsiooni (2) põhjal

$$(tf)\varphi = (t'f)\varphi \Longrightarrow (t\psi)g = (t'\psi)g,$$

järelikult g on korrektselt defineeritud st tulemus ei sõltu argumendi $s \in S$ esitusest.

Nüüd on lihtne mõista, et hulk

$$V := \{(f, t) \in B \wr T : f\varphi \text{ on } \psi\text{-kordne}\} \subseteq B \wr T,$$

on mittetühi. Olgu $(f, t), (g, u) \in V$, siis iga $x, y \in T$ korral

$$\begin{aligned} &x\psi = y\psi \Longrightarrow (xt)\psi = (yt)\psi \Longrightarrow ((xt)g)\varphi = ((yt)g)\varphi \quad \text{ja} \\ &(x(f\ {}^t g))\varphi = (xf)\varphi\,((xt)g)\varphi = (yf)\varphi\,((yt)g)\varphi = (y(f\ {}^t g))\varphi. \end{aligned}$$

Eelnevalt oleme näidanud, et sellisel juhul kujutus $(f\ {}^t g)\varphi : T \to A$ on ψ-kordne, seega hulk V on alampoolrühm.

Defineerime kujutuse

$$\omega : V \to A \wr S, \quad (f, t) \mapsto (f', t\psi),$$

kus f' on valitud nii, et $f\varphi = \psi f'$. Olgu $(f, t), (g, u) \in V$. Tähistame $(f, t)(g, u) := (h, tu)$ ehk iga $x \in T$ korral $xh = (xf)(xt)g$. Tähistame veel

$$(f', t\psi)(g', u\psi) := (k, (tu)\psi),$$

kus iga $x \in S$ korral $xk = (xf')(x(t\psi))g'$. Märgime, et iga $z \in T$ korral

$$(z\psi)k = (z\psi)f'\,((zt)\psi)g' = (zf)\varphi\,((zt)g)\varphi = (z\psi)h',$$

järelikult $k = h'$, millega oleme näidanud, et iga $(f, s), (g, t) \in V$ korral

$$((f, s)(g, t))\,\omega = (h, st)\omega = (h', (st)\psi) = (k, (st)\psi)\omega = (f, s)\omega\,(g, t)\omega$$

ehk kujutus ω on homomorfism. Näitame ka, et ω on sürjektiivne. Olgu $(f', s) \in A \wr S$. Kuna φ on sürjektiivne, siis mistahes kujutus $h : T \to A$ on φ-kordne ehk leidub kujutus $f : T \to B$ nii, et $h = f\varphi$. Samuti, ψ sürjektiivsuse tõttu leidub $t \in T$ nii, et

$s = t\psi$, seega $(f,t)\omega = (f', s)$. Kokku saame, et $A \wr S \prec B \wr T$.

Viimaks tõestame väite üldise kehtivuse. Olgu A, B, T poolrühmad, mille korral

$$A \prec B \quad \text{ja} \quad S \prec T.$$

Leiduvad alampoolrühmad $B' \subseteq B$ ja $T' \subseteq T$ ning sürjektiivsed homomorfismid $\varphi : B' \to A$ ja $\psi : T' \to S$. Siis (b) osa põhjal $A \wr S \prec B' \wr T'$ ja (a) osa põhjal $B' \wr T' \prec B \wr T$ ja transitiivsuse põhjal $A \wr S \prec B \wr T$. ■

Järeldus ([G] V.3.5). *Olgu G lõplik rühm. Siis G jagab põimikkorrutist, mis on saadud lihtsatest rühmadest, mis jagavad rühma G.*

Tõestus. Olgu G lõplik rühm. On teada, et igal lõplikul rühmal on olemas kompositsioonijada st leiduvad rühmad G_j nii, et

$$1 := G_0 \lhd G_1 \lhd G_2 \lhd \ldots \lhd G_n := G \qquad (n \in \mathbb{N})$$

kus iga $j = 1, 2, \ldots, n$ korral $G_j / G_{j-1} =: H_j$ on lihtne rühm ning iga $j = 1, \ldots, n$ korral $H_j \prec G$. Kuna $G_{j-1} \lhd G_j$, siis G_j on G_{j-1} laiendrühm H_j abil ning lause 2.2.2 põhjal iga $j = 1, 2, \ldots, n$ korral $G_j \prec G_{j-1} \wr H_j$, kusjuures lause 2.2.1 põhjal $G_0 \wr H_1 \cong H_1$. Lauset 2.2.4 rekurrentselt rakendades saame

$$\begin{aligned} G = G_n &\prec G_{n-1} \wr H_n \prec (G_{n-2} \wr H_{n-1}) \wr H_n \prec \ldots \\ &\prec (\ldots (G_0 \wr H_1) \wr H_2) \wr H_3) \wr \ldots) \wr H_n \\ &\cong H_1 \wr H_2 \wr \ldots \wr H_n. \end{aligned}$$

Transitiivsuse põhjal G jagab põimikkorrutist, mis on saadud lihtsatest rühmadest $H_1, \ldots, H_n$, mis jagavad rühma G. ■

Esitame nüüd konstruktsiooni, mida läheb vaja edaspidises. Olgu S' mingi hulk valitud nii, et $S \cap S' = \emptyset$ ja $s \mapsto s'$ on bijektsioon $S \to S'$. Tähistatakse $C(S) := S \sqcup S'$; $S \subset C(S)$ on alampoolrühm. Teised korrutised defineeritakse nii, et iga $s, t \in S$ korral

$$st' = s't' = t' \quad \text{ja} \quad s't = (st)'.$$

Lause 2.2.5. *Hulk $C(S)$ on poolrühm eelnevalt defineeritud korrutamise suhtes.*

Tõestus. Konstruktsiooni põhjal $S, S' \subset C(S)$ on alampoolrühmad. Tõepoolest, olgu $s, t, v \in S$, siis

$$s'(t'v') = s'v' = v' \quad \text{ja} \quad (s't')v' = t'v' = v'.$$

Veendume ka teiste korrutiste assotsiatiivsuses. Mistahes $s, t, v \in S$ korral

$$\begin{array}{lll}
(s't')v = t'v = (tv)' & \text{ja} & s'(t'v) = s'(tv)' = (tv)', \\
(s't)v = (st)'v = (stv)' & \text{ja} & s'(tv) = (stv)', \\
(s't)v' = (st)'v' = v' & \text{ja} & s'(tv') = s'v' = v', \\
(st)v' = v' & \text{ja} & s(tv') = sv' = v', \\
(st')v' = t'v' = v' & \text{ja} & s(t'v') = sv' = v', \\
(st')v = t'v = (tv)' & \text{ja} & s(t'v) = s(tv)' = (tv)',
\end{array}$$

millega oleme näidanud, et $C(S)$ on poolrühm. ■

Vastava eestikeelse terminoloogia puudumise tõttu nimetame poolrühma $C(S)$ poolrühma S **konstantseks laiendiks**. Lihtne on mõista, et kui S on monoid, siis $C(S)$ on monoid ühikelemendiga 1_S.

Konstantse laiendi moodustamise konstruktsioon on kooskõlas jaguvusega.

Lemma 2.2.6 ([G] V.3.6). *Olgu T poolrühm. Kui $S \prec T$, siis $C(S) \prec C(T)$.*

Tõestus. Kui $S \subseteq T$ on alampoolrühm, siis ka $C(S) \subseteq C(T)$ on alampoolrühm ja lause 2.1.1 (a) osa põhjal $C(S) \prec C(T)$.

Leidugu alampoolrühm $V \subseteq T$ ja sürjektiivne homomorfism $\varphi : V \to S$, siis $C(V) := V \sqcup V' \subseteq C(T)$ on alampoolrühm. Defineerime kujutuse

$$\psi : C(V) \to C(S), \quad x \mapsto \begin{cases} x\varphi, & x \in V, \\ (t\varphi)', & x = t' \in V' \end{cases}.$$

Olgu $t, v \in V$, $t\varphi = s$ ja $v\varphi = u$, siis $t'\psi = s'$ ja $v'\psi = u'$ ning

$$\begin{array}{lll}
(t'v')\psi = v'\psi = u' & \text{ja} & (t'\psi)\,(v'\psi) = s'u' = u', \\
(t'v)\psi = (tv)'\psi = (su)' & \text{ja} & (t'\psi)\,(v\psi) = s'u = (su)', \\
(tv')\psi = v'\psi = u' & \text{ja} & (t\psi)(v'\psi) = su' = u',
\end{array}$$

millega oleme näidanud, et ψ on homomorfism. Asjaolu, et ψ on sürjektiivne, on ilmne. Kokku saame $C(S) \prec C(T)$. ■

Potentsiaalselt on konstantse laiendi konstruktsioon teatud mõttes kooskõlas ka põimikkorrutise konstruktsiooniga. Järgnev tulemus on esitatud Grillet' monograafias [G] tulemusena V.3.7, mille tõestus ei ole ammendav.

Hüpotees 2.2.7. *Olgu A poolrühm ja S monoid. Siis $C(A \wr S) \prec C(A) \wr C(S)$.*

Tõestus. Olgu $f \in A^S$, defineerime $f' : C(S) \to A$ nii, et iga $x \in S$ korral

$$xf' = x'f' = xf.$$

Samuti defineeritakse iga $y \in C(S)$ korral konstantne kujutus

$$f'' : C(S) \to C(A), \quad y \mapsto (1f)'.$$

Defineeritakse kujutus

$$\varphi : C(A \wr S) \to C(A) \wr C(S), \quad (f, s) \mapsto (f', s) \quad \text{ja} \quad (f, s)' \mapsto (f'', s')$$

ning väidetakse, et φ on injektiivne. Olgu $f, g \in A^S$ ja $s, t \in S$ omadusega $(f, s) \neq (g, t)$. Kui $f \neq g$, siis leidub $s \in S$ omadusega

$$s'f' = sf' = sf \neq sg = sg' = s'g',$$

järelikult $(f, s)\varphi \neq (g, t)\varphi$.

Kujutuse φ definitsioonist aga ei piisa tema injektiivsuseks. Me esitame selle seisukoha toetamiseks käesoleva väite järgses märkuses vastunäite.

Näitame, et φ on homomorfism. Olgu $f, g \in A^S$ ja $s, t \in S$. Tähistame $(f, s)(g, t) := (h, st)$ ehk iga $x \in S$ korral $xh = (xf)(xs)g$. Siis:

(a) $(f, s)\varphi\,(g, t)\varphi = (f', s)(g', t) = (h', st)\varphi$, sest iga $x \in S$ korral

$$x\,(f'\ {}^{s}(g')) = (xf')(xs)g' = (xf)(xs)g = xh = xh'.$$

(b) $(f, s)\varphi\,(g, t)'\varphi = (f', s)(g'', t') = (g'', t') = (g, t)'\varphi = ((f, s)(g, t)')\varphi$, sest iga $x \in C(S)$ korral

$$x\,(f'\ {}^{s}(g'')) = (xf')(xs)g'' = (xf)(1g)' = (1g)' = xg''.$$

(c) $(f, s)'\varphi\,(g, t)\varphi = (f'', s')(g', t) = (h'', (st)') = ((f, s)(g, t))'\,\varphi$, sest iga $x \in C(S)$ korral

$$x(f''\ {}^{s'}(g')) = (xf'')(xs')g' = (1f)'(s'g') = (1f)'(sg) = ((1f)(sg))' = (1h)' = xh''.$$

(d) $(f, s)'\varphi\,(g, t)'\varphi = (f'', s')(g'', t') = (g'', t') = (g, t)'\varphi = ((f, s)'(g, t)')\varphi$,

sest iga $x \in C(S)$ korral

$$x\left(f''^{\,s'}(g'')\right) = (xf'')(xs')g'' = (1f)'(s'g'') = (1f)'(1g)' = (1g)' = xg'',$$

millega oleme näidanud, et φ on homomorfism.

Märkus.

Olgu vaatluse all kujutus φ hüpoteesi 2.2.7 tõestusest. Olgu S vähemalt kolme-elemendiline monoid ja A vähemalt kolme-elemendiline poolrühm. Näitame, et φ ei ole injektiivne elementidel

$$(f,s)', (g,s)' \in C(A \wr S).$$

Olgu $a, b, c \in A$ paarikaupa erinevad elemendid ja $1, s, t \in S$. Valime $f, g \in A^S$ järgmiselt:

$$1f = 1g = a, \quad sf = b, tf = c \quad \text{ja} \quad sg = c, tg = b.$$

Siis iga $y \in C(S)$ korral $yf'' = yg'' = a'$ ehk $f'' = g''$. Et aga $f \neq g$, siis

$$(f,s) \neq (g,s) \Longrightarrow (f,s)' \neq (g,s)' \quad \text{ja} \quad (f'', s') = (f,s)'\varphi = (g,s)'\varphi = (g'', s'),$$

millega oleme näidanud, et kujutus φ ei ole injektiivne.

Me edaspidi oletame, et hüpoteesi 2.2.7 väide siiski kehtib.

Krohn-Rhodes'i teoreem

Käesolevas peatükis lahendame bakalaureusetöö põhiülesande, milleks on osaliselt tõestada tulemus V.4.1 Grillet' monograafiast [G].

3.1 Põhiteoreemiga seonduvad tulemused

Definitsioon. Poolrühm S on **parempoolse** (**vasakpoolse**) **korrutamisega**, kui iga $x, y \in S$ korral $xy = y$ ($xy = x$).

Monoidi U_3 all peetakse silmas parempoolse korrutamisega poolrühma $\{a, b\}$, millele on väliselt lisatud ühikelement. Seega U_3 on monoid, mille korrutustabel on

U_3	a	b	1
a	a	b	a
b	a	b	b
1	a	b	1

Tähistatakse $n \in \mathbb{N}$ elemendilist vasakpoolse korrutamisega poolrühma sümboliga L_n ning n elemendilist parempoolse korrutamisega poolrühma sümboliga R_n. Lause 2.1.1 (a) osa kehtivad $L_n \prec L_n^1$ ja $R_n \prec R_n^1$.

Lemma 3.1.1 ([G] V.4.2). *Iga lõplik vasakpoolse korrutamisega poolrühm jagab lõplikku põimikkorrutist, mis on saadud monoididest U_3.*

Tõestus. Tõestame väite induktsiooniga vasakpoolse korrutamisega poolrühma L_n elementide arvu $n \in \mathbb{N}$ järgi. Paneme tähele, et $L_1^1 \prec U_3$. Tõepoolest, hulk $\{a, 1\} \subset U_3$ on alammonoid. Pole raske mõista, et kujutus

$$\varphi : \{a, 1\} \to L_1^1 := \{0, 1\}, \quad a \mapsto 0 \quad \text{ja} \quad 1 \mapsto 1$$

on isomorfism. Olgu induktiivne eeldus, et iga $k \in \mathbb{N}$, $1 \leq k < n$ korral

$$L_k^1 \prec \underbrace{U_3 \,\mathsf{w}\, U_3 \,\mathsf{w}\, \ldots \,\mathsf{w}\, U_3}_{k \text{ tegurit}}. \tag{3}$$

Näitame, et väide (3) kehtib juhul $k = n$. Selleks näitame, et $L_n^1 \prec L_{n-1}^1 \,\mathsf{w}\, L_1^1$. Olgu $a \in L_{n-1}^1$ ja defineerime kujutuse

$$f_a : L_1^1 \to L_{n-1}^1, \quad 1 \mapsto a \quad \text{ja} \quad 0 \mapsto 1.$$

Kuna iga $x \in L_1^1$ korral $x\,(f_a\ {}^0f_b) = (xf_a)(0f_b) = xf_a$, siis

$$(f_a, 0)(f_b, 0) = (f_a, 0),$$

seega hulk $\{(f_a, 0) : a \in L_{n-1}^1\} \subset L_{n-1}^1 \,\mathsf{w}\, L_1^1$ on alampoolrühm. Märgime ka, et iga $a \in L_{n-1}^1$ korral

$$(f_a, 0)(e, 1) = (e, 1)(f_a, 0) = (f_a, 0),$$

kus iga $x \in L_1^1$ korral $xe = 1$, seega element $(e, 1)$ on ühikelement ning hulk

$$T := \{(f_a, 0) : a \in L_{n-1}^1\} \cup \{(e, 1)\} \subset L_{n-1}^1 \,\mathsf{w}\, L_1^1$$

on alampoolrühm ja $L_n^1 \cong T$.

Induktiivse eelduse kohaselt väide (3) kehtib $k = n - 1$ ja $k = 1$ korral. Lausest 2.2.4 järeldub, et väide (3) kehtib $k = n$ korral ning transitiivsuse põhjal kehtib

$$L_n \prec L_n^1 \prec \underbrace{(U_3 \,\mathsf{w}\, \ldots \,\mathsf{w}\, U_3)}_{n-1 \text{ tegurit}} \,\mathsf{w}\, U_3 = \underbrace{U_3 \,\mathsf{w}\, \ldots \,\mathsf{w}\, U_3}_{n \text{ tegurit}},$$

nagu tarvis. ■

Lemma 3.1.2 ([G] V.4). *Iga lõplik parempoolse korrutamisega poolrühm jagab lõplikku põimikkorrutist, mis on saadud monoididest U_3.*

Tõestus. Olgu $R_m, m \in \mathbb{N}$ parempoolse korrutamisega lõplik poolrühm. Lihtne on mõista, et leidub $n \in \mathbb{N}$ omadusega $m \leq 2^n$. Samuti on lihtne mõista et iga parempoolse korrutamisega poolrühma suvaline alamhulk on alampoolrühm. Fikseerime parempoolse korrutamisega alampoolrühma $\{a, b\} \subset U_3$. Siis otsekorrutis

$$\underbrace{\{a, b\} \times \ldots \times \{a, b\}}_{n \text{ tegurit}} =: T$$

on mõistagi parempoolse korrutamisega poolrühm, mis sisaldab 2^n elementi. Fikseerime

suvalise m-elemendilise alamhulga $U \subseteq T$, siis $U \cong R_m$, kusjuures lause 2.1.1 põhjal

$$R_m \prec U \prec T \prec \underbrace{U_3 \times \ldots \times U_3}_{n \text{ tegurit}}.$$

Lause 2.2.3 põhjal

$$\underbrace{U_3 \times \ldots \times U_3}_{n \text{ tegurit}} \prec \underbrace{U_3 \,\mathsf{w}\, \ldots \,\mathsf{w}\, U_3}_{n \text{ tegurit}}.$$

Transitiivsuse põhjal R_m jagab lõplikku põimikkorrutist, mis on saadud monoididest U_3. ■

Definitsioon. Poolrühm S on **vasakult lihtne**, kui S sisaldab vähemalt kaks elementi ja ei sisalda mittetriviaalset vasakpoolset ideaali ehk mistahes vasakpoolse ideaali $I \subseteq S$ korral $I = S$.

Lemma 3.1.3 ([G] V.4.3). *Olgu S vähemalt kaheelemendiline lõplik poolrühm. Siis S on vasakult lihtne või S on monogeenne või $S = T \cup L$, kus $T \subset S$ on alampoolrühm ja $L \subset S$ on vasakpoolne ideaal.*

Tõestus. Ärgu olgu S vasakult lihtne ega monogeenne, siis poolrühma S lõplikuse tõttu leidub maksimaalne vasakpoolne ideaal $L \subset S$ st mistahes vasakpoolse ideaali $I \subseteq S$ korral

$$L \subset I \Longrightarrow I = S.$$

Näitame, et leidub vasakpoolne ideaal $L' \subset S$ ja alampoolrühm $T \subset S$ omadusega $S = T \cup L'$.

Iga $a \in S \setminus L$ korral hulk $S^1a \cup L$ on vasakpoolne ideaal. Vasakpoolse ideaali L maksimaalsuse tõttu $S = S^1a \cup L$. Kuna hulk S^1a on alampoolrühm, siis väide kehtib eeldusel, et leidub $a \in S \setminus L$ omadusega $S^1a \subset S$.

Olgu iga $a \in S \setminus L$ korral $S^1a = S$ ja fikseerime $a \in S \setminus L$. Siis $S = \langle a \rangle \cup Sa$, kus $\langle a \rangle \subset S$ on elemendi $a \in S$ poolt tekitatud alampoolrühm ja Sa on vasakpoolne ideaal. Kuna S ei ole monogeenne, siis $\langle a \rangle \subset S$, seega väide kehtib eeldusel, et leidub $a \in S \setminus L$ omadusega $Sa \subset S$.

Olgu iga $a \in S \setminus L$ korral $Sa = S$. Fikseerime $a \in S \setminus L$. Kuna L on vasakpoolne ideaal, siis hulk

$$K_a := \{x \in S : xa \in L\}$$

on samuti vasakpoolne ideaal poolrühmas S. Paneme tähele, et $K_a a = L$. Tõepoolest, sisalduvus $\subseteq$ kehtib triviaalselt. Teisalt, kui $y \in L$, siis eelduse $Sa = S$ kohaselt leidub $x \in S$ omadusega $xa = y \in L$, järelikult $x \in K_a$ ja $y \in K_a a$. Veelgi enam, $K_a \neq S$, sest vastasel juhul $L = K_a a = Sa = S$, mis on võimatu. Kui leidub $a \in S \setminus L$

omadusega $K_a \not\subseteq L$, siis L maksimaalsuse tõttu $L \cup K_a = S$ ja väide kehtib.

Kehtigu iga $a \in \backslash L$ korral $K \subseteq L$. Seega iga $x \in S$ ja $a \in S \setminus L$ korral kehtib implikatsioon

$$xa \in L \Longrightarrow x \in L. \tag{4}$$

Et implikatsioon (4) kehtib suvalise $a \in S \setminus L$ korral, siis mistahes $a, b \in S \setminus L$ korral $ab \in S \setminus L$, järelikult $S \setminus L \subset S$ on alampoolrühm. ■

Lemma 3.1.4 ([G] V.4.4). *Olgu S lõplik vasakult lihtne poolrühm. Siis S jagab põimikkorrutist, mis on saadud poolrühma S alamrühmast ja monoididest U_3.*

Tõestus. Näitame kõigepealt, et poolrühm S on vasakult lihtne parajasti siis, kui ta koosneb täpselt ühest $\mathscr{L}$-klassist.

Olgu S vasakult lihtne poolrühm ja olgu $L_x \subseteq S, x \in S$ tema mingi $\mathscr{L}$-klass. Poolrühma S vasakult lihtsuse tõttu iga $s \in S$ korral $S = S^1x = S^1s$. Seega iga $s \in S$ korral $s \in L_x$ ja $S \subseteq L_x$.

Teisalt, olgu $I \subseteq S$ vasakpoolne ideaal ja üldisust kitsendamata $S = L_x$, kus $x \in I$. Siis iga $s \in S$ korral leidub $u \in S^1$ omadusega $s = ux \in I$, seega $I = S$ ehk S on vasakult lihtne.

Kuna S on lõplik, siis lause 1.4.1 põhjal leidub idempotent poolrühmas S. Veendume, et hulk $E(S)$ on vasakpoolse korrutamisega alampoolrühm. Tõepoolest, olgu $e, f \in E(S)$ idempotendid. Eelneva põhjal $S = L_f$, seega leidub $s \in S^1$ omadusega $e = sf$ ja

$$ef = (sf)f = s(ff) = sf = e.$$

Järgnev lõik põhineb Howie raamatul [H] (Ülesanne 2.6.6).

Olgu $e \in E(S)$. Analoogiliselt saab ka veenduda järgmises asjaolus:

$$(\forall x \in S)\,(xe = x)\,. \tag{5}$$

Paneme tähele, et $eS \subseteq S$ on rühm ühikelemendiga e. Pole raske mõista, et $eS = H_e$. Lause 1.1.5 põhjal H_e on poolrühma S alamrühm. Fikseerime $f \in E(S)$, siis kujutus

$$\varphi : E(S) \times H_f \to S, \quad (e, h) \mapsto eh$$

on isomorfism. Tõepoolest, olgu $e, e' \in E(S)$ ja $h, h' \in H_f$ omadusega $eh = e'h'$. Kuna klassid $H_x, x \in E(S)$ on paarikaupa lõikumatud, siis saame

$$eh \in eS = H_e \quad \text{ja} \quad e'h' \in e'S = H_{e'},$$

mis on võimalik juhul kui $e = e'$. Olgu siis $eh = eh'$. Et kehtib fakt (5) ja H_f on

rühm, siis võttes selles rühmas elemendi h pöördelemendi h^{-1} saame, et

$$h^{-1}(eh) = h^{-1}(eh') \Longrightarrow (h^{-1}e)h = (h^{-1}e)h' \Longrightarrow f = h^{-1}h' \\ \Longrightarrow h = hf = hh^{-1}h' = fh' = h',$$

seega $(e,h) = (e',h')$ ning oleme näidanud, et φ on injektiivne. Kui $s \in S$, siis leidub üheselt määratud $e \in E(S)$ nii, et $s \in H_e$. Kuna $H_e = H_{ef}$, siis leidub $t \in S^1$ omadusega $s = e(ft)$. Kui $t = 1$, siis $(e,f)\varphi = s$. Teisalt, kui $t \in S$, siis leidub $x \in E(S)$ omadusega $t \in H_x$, järelikult $ft \in H_f$ ja $(e,ft)\varphi = s$, millega oleme näidanud, et φ on sürjektiivne. Näitamaks, et φ on homomorfism märgime, et

$$((e,h)(e',h'))\,\varphi = (ee')(hh') = ehh' = e(hfe')h' = (eh)(e'h') = (e,h)\varphi\,(e',h')\varphi.$$

Lause 3.1.1 põhjal lõplik poolrühm $E(S)$ jagab põimikkorrutist, mis on saadud monoididest U_3. Lause 2.2.4 põhjal poolrühm $E(S)\,\mathsf{w}\,H_f$ jagab põimikkorrutist, mis on saadud rühmast H_f ja monoididest U_3. Lause 2.2.3 põhjal $E(S) \times H_f \prec E(S)\,\mathsf{w}\,H_f$. Transitiivsuse põhjal S jagab põimikkorrutist, mis on saadud maksimaalsest alamrühmast $H_f \subseteq S$ ja monoididest U_3. ■

Lemma 3.1.5 ([G] V.4.5). *Iga lõplik monogeenne monoid S jagab põimikkorrutist, mis on saadud monoidi S alamrühmast G ja monoididest U_3.*

Tõestus. Olgu S lõplik monogeenne monoid. Siis $S = \langle a; a^m = a^{m+n}\rangle$, kus $m,n \in \mathbb{N}$ on vähimad sellised naturaalarvud, mille korral kehtib $a^m = a^{m+n}$. Monoid S sisaldab rühma

$$G = \left\{a^m, a^{m+1}, \ldots, a^{m+n-1}\right\}$$

(vt [K2] VI.5). Seega monoid S on rühma $G \subseteq S$ Cliffordi laiend monogeense monoidi $C_m := \langle b; b^m = b^{m+1}\rangle$ abil. Tõepoolest, pole raske mõista, et $G \subseteq S$ on ideaal, kusjuures Rees'i faktorpoolrühm S/G on samastatav monoidiga C_m.

Olgu e rühma G ühikelement. Defineerime kujutuse

$$\eta : S \to S, \quad s \mapsto se,$$

kusjuures $(s\eta)\eta = (se)\eta = se = s\eta$, seega η on idempotentne teisendus. Kuna $e \in G$, siis $e = a^u$, kus $u \geq m$, järelikult iga $s \in S$ korral korrutis $se \in G$. Teisalt, iga $g \in G$ korral $g = ge = g\eta$, seega $S\eta = G$. Olgu $s,t \in S$, siis

$$(st)\eta = (st)e = s(te) = s(t\eta) = s(e(t\eta)) = (s\eta)(t\eta),$$

seega η on retraktsioon, mille korral $S\eta = G$. Lause 1.3.1 põhjal $S/\ker\eta \cong G$.

Olgu $\mathscr{F}$ ideaali G poolt tekitatud Rees'i kongruents. Lihtne on mõista, et $\ker\eta \cap \mathscr{F} = \mathscr{E}$. Lause 1.3.3 põhjal poolrühm ${}^{S}\!/_{\mathscr{F}} \cap \ker\eta$ on alamotsekorrutis poolrühmas ${}^{S}\!/_{\mathscr{F}} \times {}^{S}\!/_{\ker\eta}$. Et alamotsekorrutis on alampoolrühm, siis lause 2.1.1 (a) osa põhjal saame, et

$$S \cong {}^{S}\!/_{\mathscr{E}} = {}^{S}\!/_{\mathscr{F}} \cap \ker\eta \prec {}^{S}\!/_{\mathscr{F}} \times {}^{S}\!/_{\ker\eta} \cong C_m \times G.$$

Lause 2.2.3 ja transitiivsuse põhjal $S \prec C_m \,\mathsf{w}\, G$.

Lihtne on mõista, et $C_1 := \{0, 1\}$ jagab monoidi U_3. Näitame, et iga $m \in \mathbb{N}, m > 1$ korral C_m on isomorfne poolrühma $C_{m-1} \,\mathsf{w}\, C_1$ mingi alampoolrühmaga.

Defineerime iga $k \in \mathbb{N}$ korral kujutuse

$$f_k : C_1 \to C_{m-1}, \quad 1 \mapsto a^{k-1} \quad \text{ja} \quad 0 \mapsto a^k,$$

kus kokkuleppeliselt loeme, et $a^0 = 1$. Kui mingi $k \in \mathbb{N}$ korral $(f, 0)^k = (f_k, 0)$, siis

$$(f, 0)^{k+1} = (f_k, 0)(f, 0) = \big(f_k\ {}^0 f, 0\big) = (f_{k+1}, 0).$$

Järelikult $(f, 0)^{m+1} = (f, 0)^m \neq (f, 0)^{m-1}$ ja monogeensed monoidid

$$\langle (f, 0); (f, 0)^{m+1} = (f, 0)^m \rangle \subseteq C_{m-1} \,\mathsf{w}\, C_1 \quad \text{ja} \quad C_m$$

on isomorfsed. Lause 2.1.1 põhjal $C_m \prec C_{m-1} \,\mathsf{w}\, C_1$.

Rekurrentselt lause 2.2.4 väidet kasutades, saame

$$\begin{aligned} S &\prec C_m \,\mathsf{w}\, G \prec (C_{m-1} \,\mathsf{w}\, C_1) \,\mathsf{w}\, G \prec \ldots \prec (\ldots (C_1 \,\mathsf{w}\, C_1) \,\mathsf{w}\, C_1) \,\mathsf{w}\, \ldots) \,\mathsf{w}\, C_1) \,\mathsf{w}\, G \\ &\prec \underbrace{U_3 \,\mathsf{w}\, \ldots \,\mathsf{w}\, U_3}_{m \text{ tegurit}} \,\mathsf{w}\, G. \end{aligned}$$

Transitiivsuse põhjal S jagab lõplikku põimikkorrutist, mis on saadud monoididest U_3 ja monoidi S alamrühmast G. ■

Lemma 3.1.6 ([G] V.4.6). *Olgu $S = T \cup L$, kus $T \subseteq S$ on alampoolrühm ja $L \subseteq S$ on vasakpoolne ideaal. Siis $S \prec L^1 \,\mathsf{w}\, C(T^1)$.*

Tõestus. Defineerime $c : C(T^1) \to L^1$ nii, et iga $x \in T^1$ korral $xc = x'c = 1$. Olgu iga $a \in L$ korral $f_a : C(T^1) \to L^1$ defineeritud nii, et iga $x \in T^1$ korral $xf_a = x'f_a = xa \in L$. Siis iga $a, b \in L$ ja iga $t, u \in T^1$ korral:

(a) $(c,t)(c,u) = (c\ {}^t c, tu) = (c, tu)$, sest iga $x \in C(T^1)$ korral

$$x\left(c\ {}^t c\right) = (xc)(xt)c = 1 = xc.$$

(b) $(c,t)(f_a,u') = (f_{ta},u')$, sest iga $x \in T^1$ korral

$$x\left(c\ {}^t f_a\right) = (xc)(xt)f_a = 1xta = xf_{ta}.$$

(c) $(f_a,t')(c,u) = (f_a,(tu)')$, sest iga $x \in T^1$ korral

$$x\left(f_a\ {}^{t'} c\right) = (xf_a)(xt')c = (xf_a)1 = xf_a.$$

(d) $(f_a,t')(f_b,u') = (f_{atb},u')$, sest iga $x \in T^1$ korral

$$x\left(f_a\ {}^{t'} f_b\right) = (xf_a)(xt')f_b = (xf_a)(t'f_b) = xatb = xf_{atb}.$$

Järelikult hulk

$$V := \left\{(f_a,t') : a \in L, t \in T^1\right\} \cup \left\{(c,t) : t \in T^1\right\} \subseteq L^1 \wr C(T^1)$$

on alampoolrühm. Defineerime kujutuse

$$\varphi : V \to S, \quad (c,t) \mapsto t \quad \text{ja} \quad (f_a,t') \mapsto at,$$

siis (a),(b),(c) ja (d) osa põhjal oleme näidanud, et φ on homomorfism. Olgu $s \in T \cup L$ suvaline. Kui $s \in T$, siis $(c,s)\varphi = s$ ja kui $s \in L$, siis $(f_s,1)\varphi = s$, millega oleme näidanud, et φ on sürjektiivne. ■

Lemma 3.1.7 ([G] V.4.7). *Olgu S lõplik monoid ja G monoidi S pööratavatest elementidest moodustatud alamrühm. Siis hulk $I := S \setminus G$ on ideaal monoidis S ja $S \prec I^1 \wr G$.*

Tõestus. Kuna G on maksimaalne alamrühm ja poolrühma maksimaalsed alamrühmad on idempotenti sisaldavad $\mathscr{H}$-klassid, siis $G = H_1$. Lause 1.4.5 põhjal hulk I on ideaal monoidis S. Defineerime iga $s \in I^1$ korral kujutuse

$$\hat{s} : G \to I^1, \quad x \mapsto xsx^{-1}$$

ning juhul $s = 1$ on tegemist kujutusega

$$\hat{1} : G \to I^1, \quad x \mapsto 1.$$

Tähistame

$$V := \left\{(\hat{s}, g) : s \in I^1, g \in G\right\} \subseteq I^1 \wr G.$$

Olgu $s, t \in I^1$ ja $g, h \in G$, siis iga $x \in G$ korral

$$x\left(\hat{s}\ {}^{g}\hat{t}\right) = (x\hat{s})(xg)\hat{t} = (xsx^{-1})(xg)t(xg)^{-1} = xsgtg^{-1}x^{-1} = x\hat{u},$$

kus $u := sgtg^{-1} \in I$, seega $(\hat{s}, g)(\hat{t}, h) = (\hat{u}, gh)$ ja $V \subseteq I^1 \wr G$ on alampoolrühm. Defineerime kujutuse

$$\varphi : V \to S, \quad (\hat{s}, g) \mapsto sg,$$

kusjuures paneme tähele, et kui $\hat{s} = \hat{t}$, siis $s = 1\hat{s} = 1\hat{t} = t$, seega φ on korrektselt defineeritud. Kuna $sgt = ug$, siis

$$((\hat{s}, g)(\hat{t}, h))\varphi = \left(\hat{s}\ {}^{g}\hat{t}, gh\right)\varphi = (\hat{u}, gh) = (ug)h = (sg)(th) = (\hat{s}, g)\varphi\,(\hat{t}, h)\varphi,$$

millega oleme näidanud, et φ on homomorfism. Et iga $s \in S$ korral $(\hat{1}, s)\varphi = s$ või $(\hat{s}, 1)\varphi = s$, siis φ on sürjektiivne. Kokku saame, et $S \prec I^1 \wr G$. ■

Leppisime kokku aktsepteerida hüpotees 2.2.7 väite õigsust. Sellegipoolest, järgmine lemma on võetav vaid hüpoteesina.

Lemma 3.1.8 ([G] V.4.8). *Kui lõplik poolrühm S jagab põimikkorrutist, mis on saadud rühmadest ja monoididest U_3, siis ka poolrühm $C(S)$ jagab põimikkorrutist, mis on saadud samadest rühmadest ja monoididest U_3.*

Tõestus. Jagagu poolrühm S põimikkorrutist, mis on saadud rühmadest G_j ja monoididest U_3. Olgu konkreetsuse mõttes järgmine olukord:

$$S \prec G_1 \wr U_3 \wr \ldots \wr G_{n-1} \wr U_3 \wr G_n \qquad (n \in \mathbb{N})$$

Esitus ei pea muidugi olema täpselt selline. Märgime aga, et rühmi G_j ja monoide U_3 on kindlasti lõplik kogus, sest S on lõplik hulk. Lemma 2.2.6 põhjal poolrühm $C(S)$ jagab eelnimetatud põimikkorrutise konstantset laiendit, kusjuures hüpotees 2.2.7 väidet rekurrentselt rakendades saame, et

$$C(S) \prec C\left(G_1 \wr U_3 \wr \ldots \wr G_n \wr U_3\right) \prec C(G_1) \wr C(U_3) \wr \ldots \wr C(G_n) \wr C(U_3),$$

kus hulgad $C(G_j)$ ja $C(U_3)$ on monoidid. Lihtne on mõista, et $C(U_3)$ on parempoolse korrutamisega poolrühm, millele on väliselt lisatud ühikelement, seega lemma 3.1.2 põhjal $C(U_3)$ jagab põimikkorrutist, mis on saadud monoididest U_3.

Iga rühm G_j koosneb täpselt monoidi $C(G_j)$ pööratavatest elementidest. Lemma 3.1.7 põhjal, iga $j = 1, \ldots, n$ korral, hulk $I_j := C(G_j) \setminus G_j$ on ideaal monoidis

$C(G_j)$ ja $C(G_j) \prec I_j^1 \,\mathsf{w}\, G_j$. Kuna $I_j = G'_j$, siis I_j on parempoolse korrutamisega poolrühm ning lemma 3.1.1 järel tehtud märkuse põhjal I_j^1 jagab põimikkorrutist, mis on saadud monoididest U_3. Lemma 3.1.7 ja lause 2.2.4 põhjal monoid $C(G_j)$ jagab põimikkorrutist, mis on saadud rühmast G_j ja monoididest U_3. Lause 2.2.4 väite ja transitiivsuse põhjal $C(S)$ jagab põimikkorrutist, mis on saadud rühmadest G_j ja monoididest U_3.

3.2 Põhiteoreemi tõestus

Nüüd oleme valmis tõestama Krohn-Rhodes'i teoreemi. Tõestus viiakse läbi induktsiooniga lõpliku poolrühma elementide arvu n järgi. Tsentraalseks osutub lemma 3.1.3 väide. Olgu veel kord esitatud põhiteoreemi sõnastus.

Teoreem (Krohn-Rhodes). *Iga lõplik poolrühm S jagab lõplikku põimikkorrutist, mis on saadud monoididest U_3 või lihtsatest rühmadest, mis jagavad poolrühma S.*

Põhiteoreemi tõestus. Kuna $S \prec S^1$, siis üldisust kitsendamata olgu S lõplik monoid.

(a) Kui S on rühm, siis lausest 2.2.4 tehtud järelduse põhjal S jagab põimikkorrutist, mis on saadud rühma S kompositsioonijada faktoritest, mis on lihtsad rühmad, mis jagavad S.

(b) Kui S on ühikelemendiga vasakult lihtne poolrühm, siis lemma 3.1.4 põhjal S jagab põimikkorrutist, mis on saadud S maksimaalsest alamrühmast G ja vasakpoolse korrutamisega poolrühmast L. Osa (a) põhjal teoreemi väide kehtib rühma G korral. Lause 3.1.1 põhjal L jagab põimikkorrutist, mis on saadud monoididest U_3. Teoreemi väide kehtib monoidi S korral lause 2.2.4 ja transitiivsuse põhjal.

(c) Kui S on monogeenne monoid, siis lemma 3.1.5 põhjal S jagab põimikkorrutist, mis on saadud monoidi S alamrühmast G ja monoididest U_3. Sarnaselt (a) ja (b) osades arutletule, monoid S jagab põimikkorrutist, mis on saadud rühma G kompositsioonijada faktoritest ja monoididest U_3.

Oletame nüüd, et $S \neq \{1\}$, S ei ole rühm, S ei ole vasakult lihtne poolrühm ja S ei ole monogeenne monoid. Kehtigu induktiivne eeldus, et teoreemi väide kehtib iga $1 < k < n$ elemendilise monoidi korral. Olgu G rühm, mis koosneb n-elemendilise monoidi S pööratavatest elementidest.

Kui $G = \{1\}$, siis $S' := S \setminus \{1\} \subset S$ on alampoolrühm ja lemma 3.1.3 põhjal $S' = T \cup L$, kus $T \subset S'$ on alampoolrühm ja $L \subset S'$ on vasakpoolne ideaal. Siis

$S = T^1 \cup L$ kus $T^1 \subset S$ ja $L \subset S$. Kui G ei ole triviaalne rühm, siis lause 1.4.5 põhjal $S \setminus G$ on ideaal monoidis S ja $G \subset S$ on alammonoid.

Oleme näidanud, et $S = T \cup L$, kus $T \subset S$ on alammonoid ja $L \subset S$ on vasakpoolne ideaal. Lemma 3.1.6 põhjal $S \prec L^1 \,\mathsf{w}\, C(T)$. Induktiivse eelduse põhjal teoreemi väide kehtib alammonoidide L^1 ja T korral. Lemma 3.1.8 põhjal teoreemi väide kehtib monoidi $C(T)$ korral ning lause 2.2.4 ja transitiivsuse põhjal monoidi S korral.

Kirjandus

[G] P. A. Grillet, *Semigroups: An Introduction to the Structure Theory*, Tulane Ülikool, New York, 1995

[K1] M. Kilp, *Algebra I*, Tartu, 1998

[K2] M. Kilp, *Algebra II*, Tartu, 1998

[H] J. M. Howie, *Fundamentals of Semigroup Theory*, Clarendon Press, 1995

[KRA] K. Krohn, J. Rhodes, American Mathematical Society, *Algebraic theory of machines. I. Prime decomposition theorem for finite semigroups and machines*, 1965
http://dx.doi.org/10.2307/1994127

[KRT] Vikipeedia, vaba entsüklopeedia 2016, *Krohn-Rhodes theory*
https://en.wikipedia.org/wiki/Krohn_Rhodes_theory

Litsents

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Alvin Lepik,

(1) annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose

"Poolrühmade põimikkorrutis ja Krohn-Rhodes'i teoreem",

mille juhendaja on Valdis Laan,

- reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

- üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace'i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

(2) olen teadlik, et punktis (1) nimetataud õigused jäävad alles ka autorile.

(3) kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, **11.05.2017**